

Configuration de l'accès sécurisé pour l'évaluation de la position de RA-VPNaaS avec ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configuration d'accès sécurisé](#)

[Configurer le groupe Radius sur les pools IP](#)

[Configurez votre profil VPN pour utiliser ISE](#)

[Paramètres généraux](#)

[Authentification, autorisation et administration \(AAA\)](#)

[Orientation Du Trafic](#)

[Configuration du client sécurisé Cisco](#)

[Configurations ISE](#)

[Configurer la liste des périphériques réseau](#)

[Configurer un groupe](#)

[Configurer l'utilisateur local](#)

[Configurer le jeu de stratégies](#)

[Configurer l'authentification et l'autorisation du jeu de stratégies](#)

[Configuration des utilisateurs de Radius Local ou Active Directory](#)

[Configuration de la position ISE](#)

[Configuration des conditions de posture](#)

[Configuration des exigences de posture](#)

[Configurer la politique de posture](#)

[Configurer le provisionnement client](#)

[Configurer la politique de provisionnement client](#)

[Créer les profils d'autorisation](#)

[Configurer le jeu de stratégies de position](#)

[Vérifier](#)

[Validation de posture](#)

[Connexion sur l'ordinateur](#)

[Comment collecter les journaux dans ISE](#)

[Conformité](#)

[Non-conformité](#)

[Premiers pas avec l'accès sécurisé et l'intégration ISE](#)

[Dépannage](#)

[Téléchargement des journaux de débogage de la position ISE](#)

Introduction

Ce document décrit comment configurer l'évaluation de position pour les utilisateurs VPN d'accès à distance avec Identity Service Engine (ISE) et Secure Access.

Conditions préalables

- [Configurer le provisionnement utilisateur](#)
- Cisco ISE connecté à Secure Access via le tunnel

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- [Identity Service Engine](#)
- [Accès sécurisé](#)
- [Client sécurisé Cisco](#)
- Posture ISE
- Authentification, autorisation et administration (AAA)

Composants utilisés

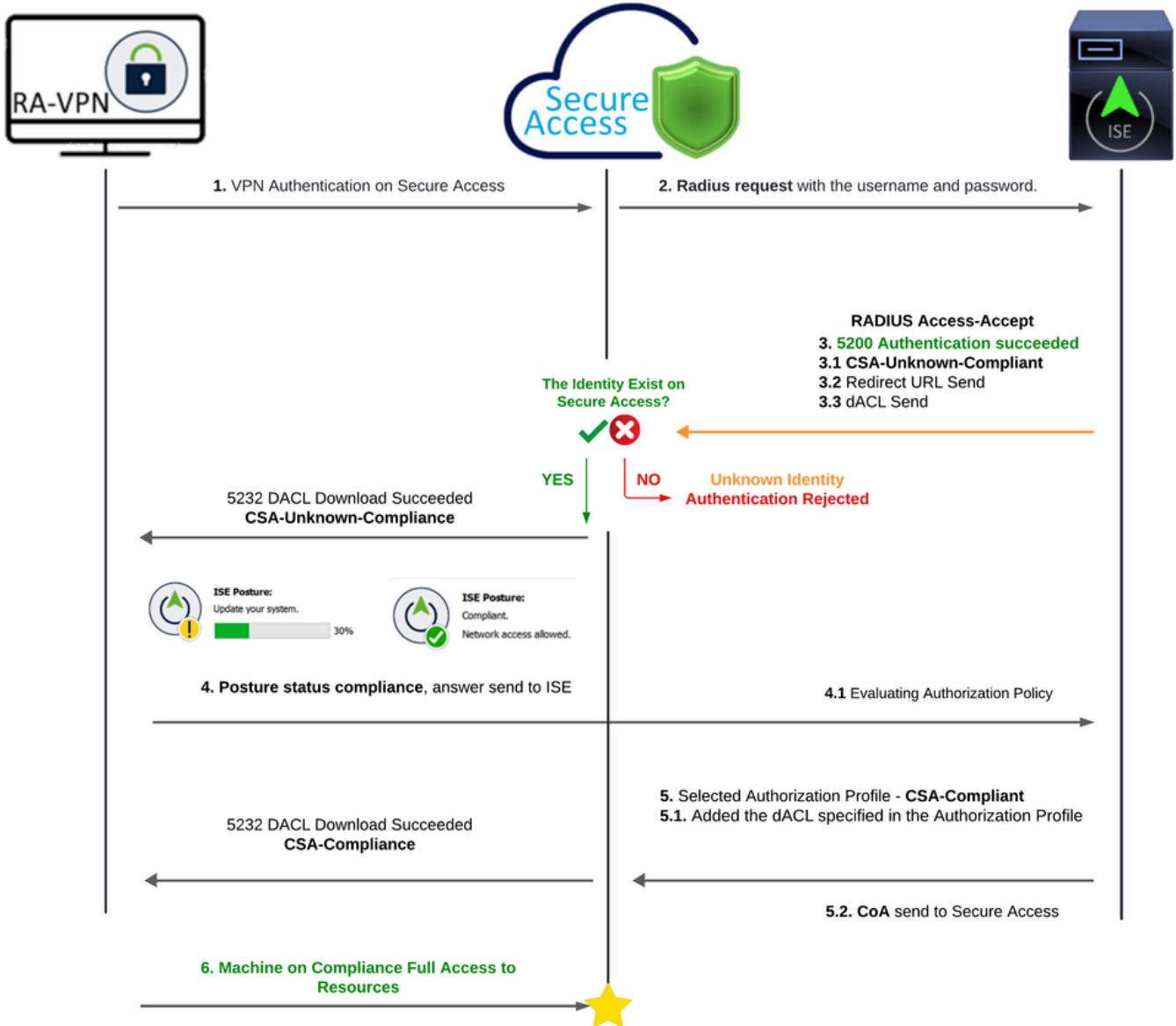
Les informations contenues dans ce document sont basées sur :

- Identity Service Engine (ISE) version 3.3, correctif 1
- Accès sécurisé
- Client sécurisé Cisco - Anyconnect VPN Version 5.1.2.42

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

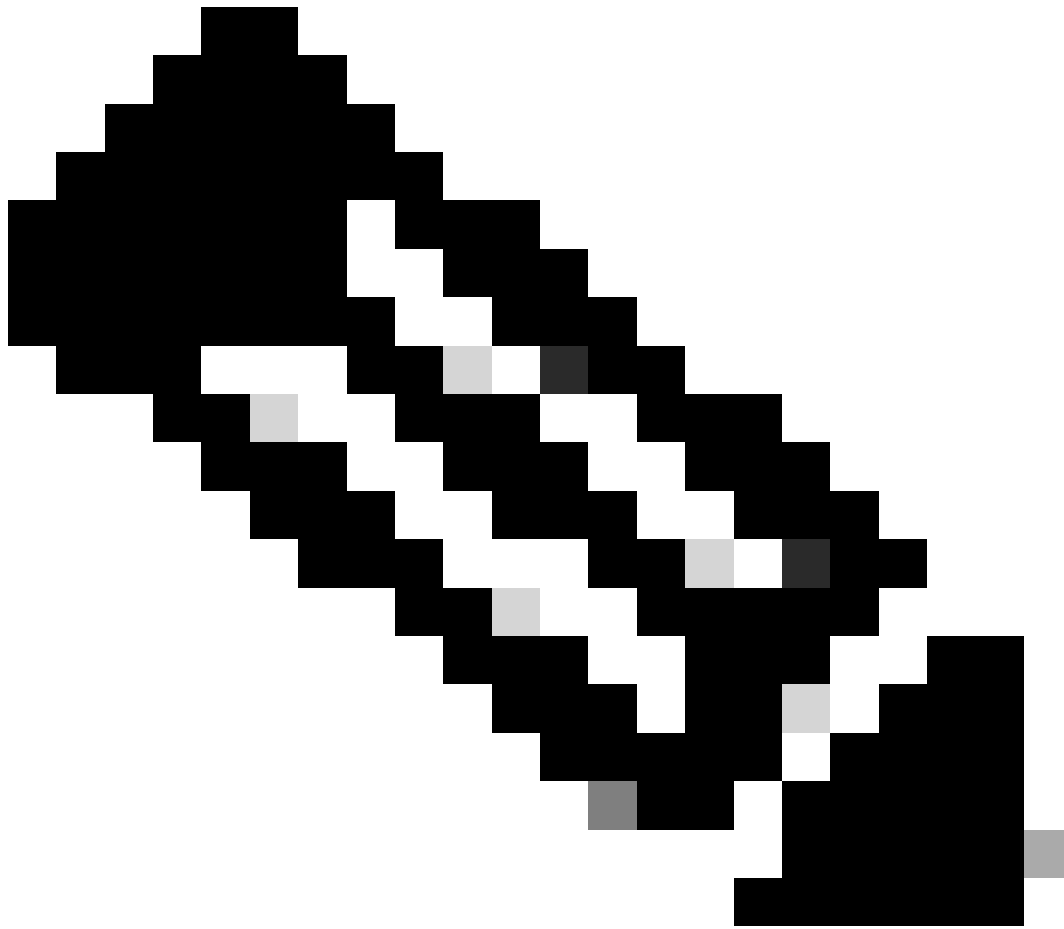
vpnuser@ciscospt.es



Accès sécurisé - ISE - Schéma

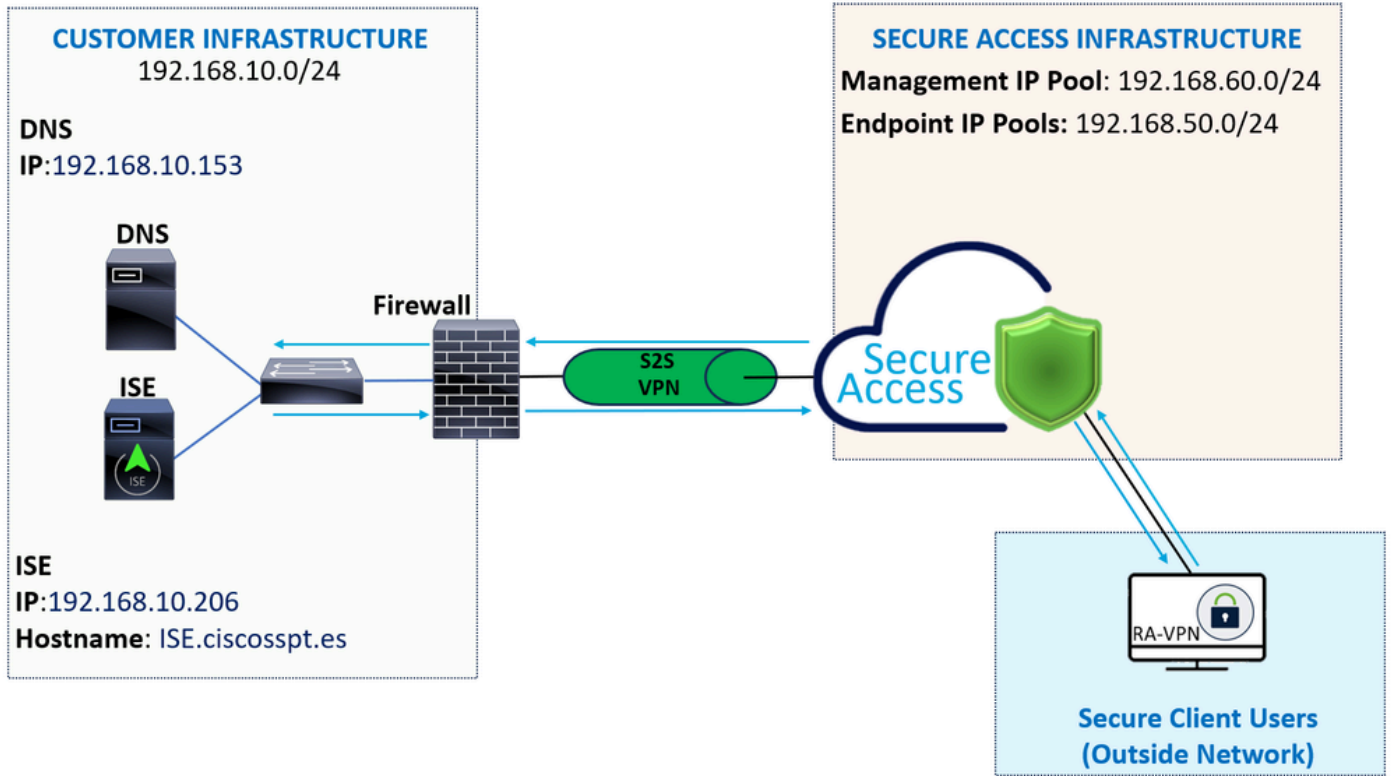
L'intégration de Cisco Secure Access avec Identity Services Engine (ISE) offre une approche de sécurité complète, qui tire parti de différents protocoles d'authentification, notamment MS-CHAPv2, pour sécuriser les connexions. Cisco Secure Access, avec sa solution avancée Security Service Edge (SSE), améliore la connectivité sécurisée dans les environnements hyperdistribués, offrant des fonctionnalités telles que VPN as a Service (VPNaaS), qui peuvent être protégées à l'aide des fonctionnalités ISE.

Cette intégration permet un accès transparent et sécurisé, permettant aux utilisateurs de se connecter à n'importe quelle application, n'importe où, avec des performances et une sécurité optimisées. L'utilisation des fonctionnalités avancées de Cisco ISE, telles que l'évaluation de la posture, renforce encore ce modèle de sécurité en évaluant la conformité des PC par rapport aux politiques internes de l'utilisateur avant d'autoriser l'accès. Cela garantit que seuls les périphériques répondant aux exigences de sécurité de l'entreprise peuvent accéder aux ressources réseau, réduisant ainsi le risque de vulnérabilités.



Remarque : pour configurer l'intégration RADIUS, vous devez vous assurer que vous avez une communication entre les deux plates-formes.

Diagramme du réseau



Configurer



Remarque : avant de commencer le processus de configuration, vous devez effectuer les [premières étapes avec Secure Access et l'intégration ISE](#).

Configuration d'accès sécurisé

Configurer le groupe Radius sur les pools IP

Pour configurer le profil VPN à l'aide de Radius, procédez comme suit :

Accédez à votre tableau de [bord d'accès sécurisé](#).



- Cliquez sur **Connect > Enduser Connectivity > Virtual Private Network**
 - Sous votre configuration de pool (**Manage IP Pools**), cliquez sur **Manage**

Manage IP Pools

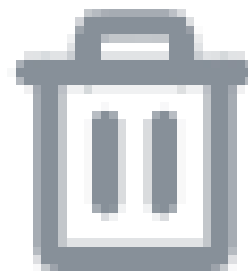
Manage

2 Regions mapped

- Sélectionnez le **IP Pool Region** et configurez le **Radius Server**

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- Cliquez sur le crayon pour le modifier



- À présent, dans la liste déroulante de configuration de la section IP Pool, sous **Radius Group (Optional)**
- Cliquer Add RADIUS Group

RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



No RADIUS groups created

Add RADIUS Group

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings



RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×



+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

Group Name: configurez un nom pour votre intégration ISE dans Secure Access

- **AAA method**

- **Authentication:** cochez la case pour **Authentication** et sélectionnez le port, par défaut, 1812

- Si votre authentification nécessite une case à cocher, Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2) cochez-la

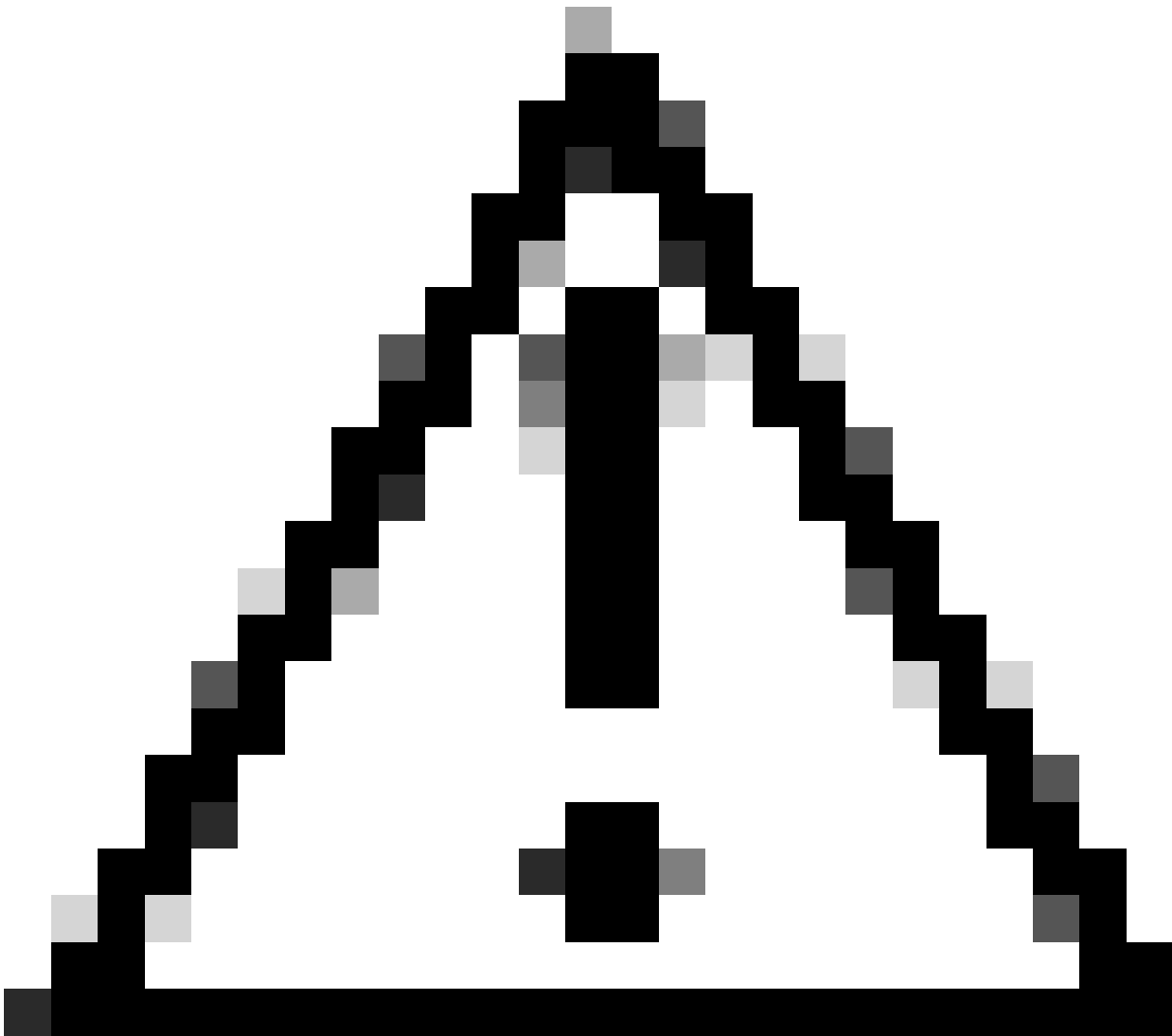
- **Authorization:** cochez la case pour Authorization et sélectionnez le port, par défaut, est 1812

- Cochez la case pour **Authorization mode Only Change of Authorization (CoA) mode** et pour autoriser la position et les modifications depuis ISE

- **Accounting:** cochez la case Autorisation et sélectionnez le port 1813 par défaut

- Choisir **Single or Simultaneous** (en mode unique, les données de comptabilité sont envoyées à un seul serveur. En mode simultané, les données de gestion des comptes à tous les serveurs du groupe)

- Cochez la case pour **Accounting update** activer la génération périodique de messages RADIUS Interim-accounting-update.



Attention : lorsque les Authentication et les **Authorization** méthodes sont sélectionnées, le même port doit être utilisé.

-
- Ensuite, vous devez configurer l' **RADIUS Servers** (ISE) qui est utilisé pour authentifier via AAA dans la section **RADIUS Servers**:
 - Cliquez sur + Add

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

#	Server Name	IP Address
---	-------------	------------

- Configurez ensuite les options suivantes :

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

Password

Cancel

Save & Add server

Save

- **Server Name:** configurez un nom pour identifier votre serveur ISE.
 - **IP Address:** configurez l'adresse IP de votre périphérique Cisco ISE accessible via l'accès sécurisé
 - **Secret Key:** configurez votre clé secrète RADIUS
 - **Password:** configurez votre mot de passe Radius
-
- Cliquez sur **Save** et attribuez votre serveur Radius sous l'Assign Server option et sélectionnez votre serveur ISE :

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- Cliquez à **Save** nouveau pour enregistrer la configuration terminée

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

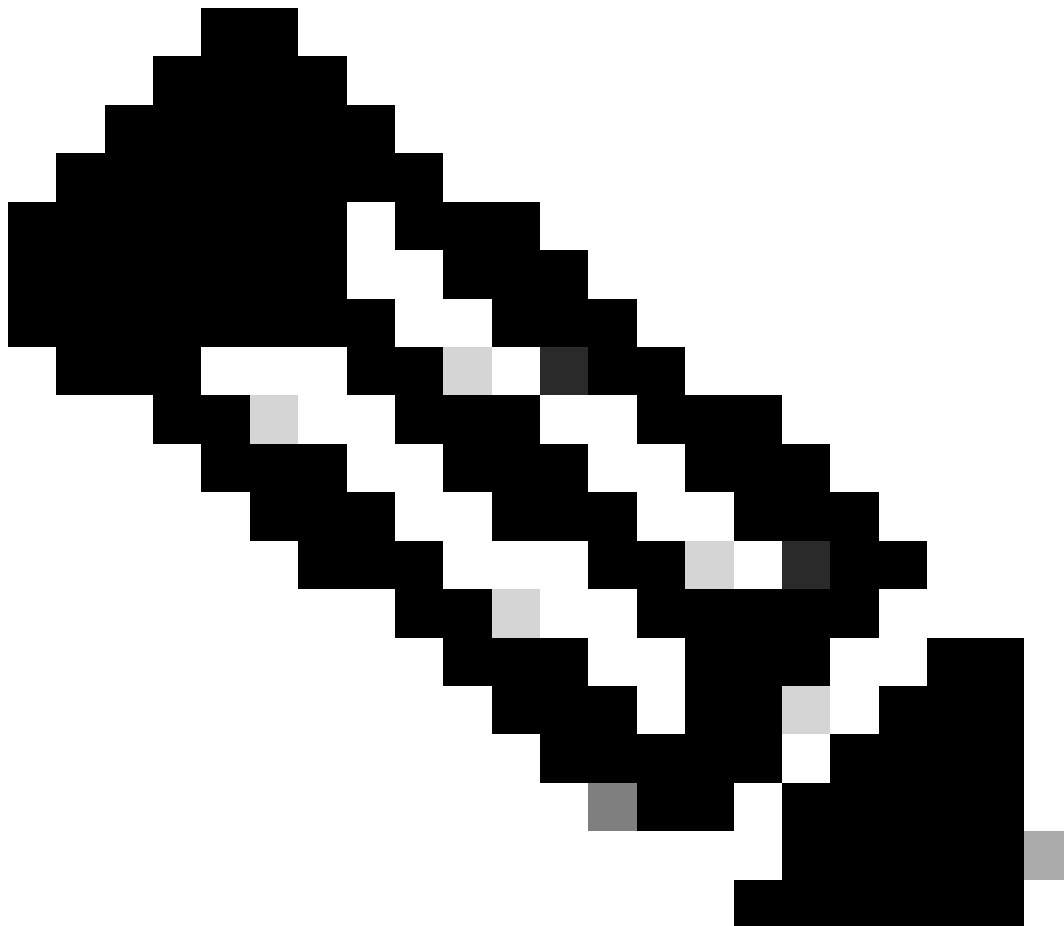
Assign servers

ISE_CSA ×

+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

- **Protocols:** Choisir **Radius**
 - **Map authentication groups to regions:** choisissez les régions et choisissez votre **Radius Groups**
-
- Cliquer **Next**



Remarque : vous devez cocher toutes les régions et sélectionner les groupes de rayons si vous avez plusieurs régions. Si vous ne le faites pas, votre **Next** bouton est grisé.

Après avoir configuré toutes les parties d'authentification, passez à l'autorisation.

Autorisation

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

Enable Radius Authorization
Use defaults or customize groups to map to regions

Select one group for all regions + Group

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)

< Cancel Back Next

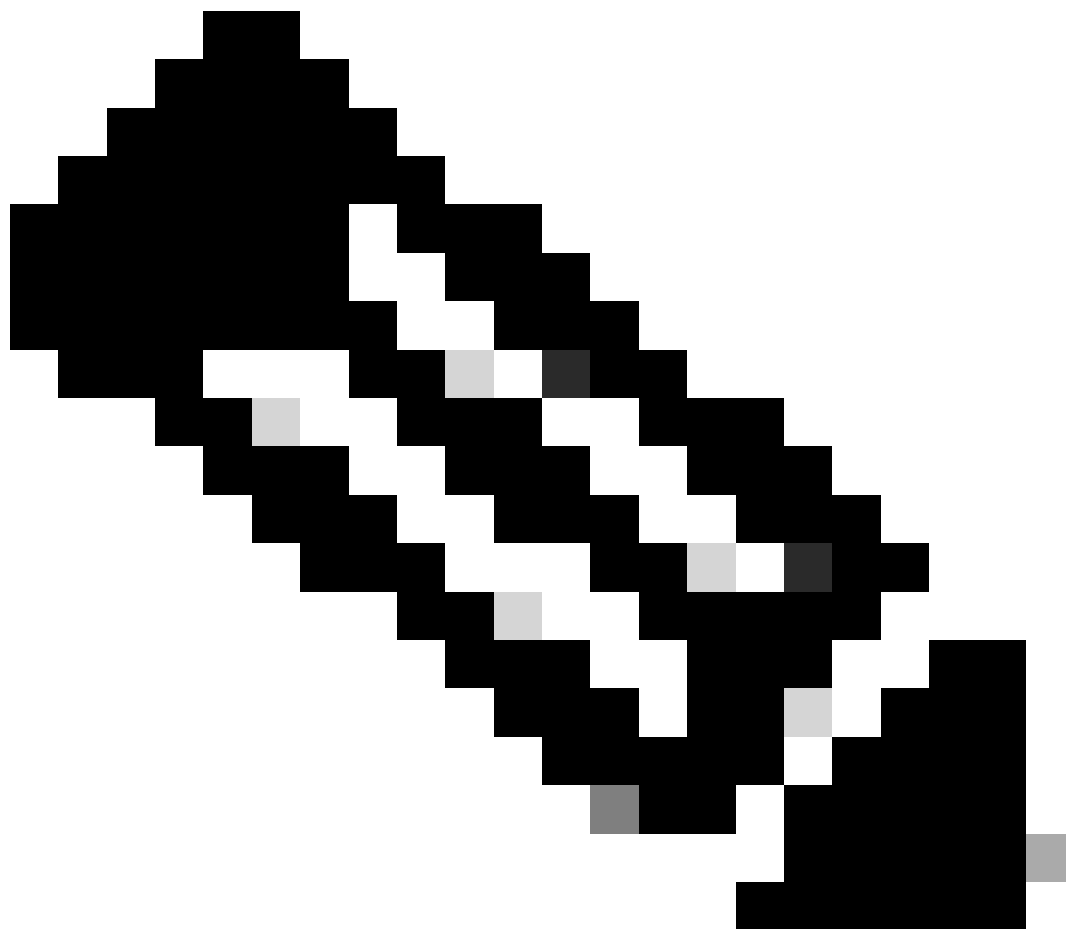
- **Authorization**

- **Enable Radius Authorization:** cochez la case pour activer l'autorisation radius.

- **Sélectionnez un groupe pour toutes les régions :** cochez la case pour utiliser un serveur RADIUS spécifique pour tous les pools d'accès à distance - réseau privé virtuel (RA-VPN) ou définissez-le séparément pour chaque pool

- Cliquer **Next**

Après avoir configuré l'ensemble de la **Authorization** pièce, passez à l' **Accounting**.



Remarque : si vous n'activez pas **Radio Authorization**, la posture ne peut pas fonctionner.

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization Accounting

Enable Radius Accounting
Use defaults or customize groups to map to regions

Select one group for all regions + Group

ISE_CSA ▼

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA ▼
RA VPN 1	192.168.60.0/24	ISE_CSA (default) ▼



Cancel

Back

Next

- **Accounting**
 - **Map Authorization groups to regions:** choisissez les régions et choisissez votre **Radius Groups**

- Cliquer **Next**

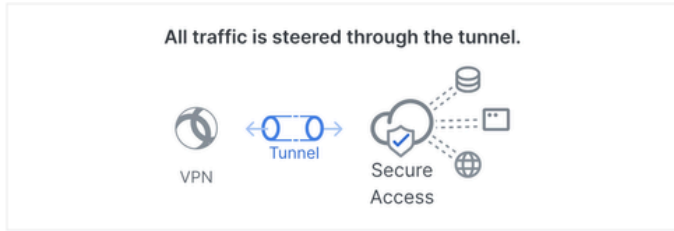
After you have done configured the Authentication, Authorization and Accounting veuillez poursuivre avec Traffic Steering.

Orientation Du Trafic

Sous l'orientation du trafic, vous devez configurer le type de communication via l'accès sécurisé.

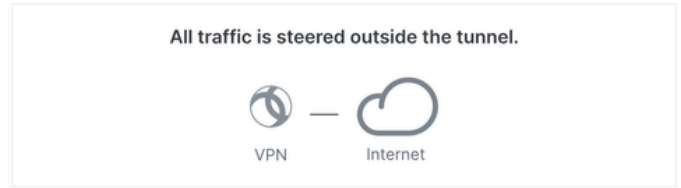
Tunnel Mode

Connect to Secure Access



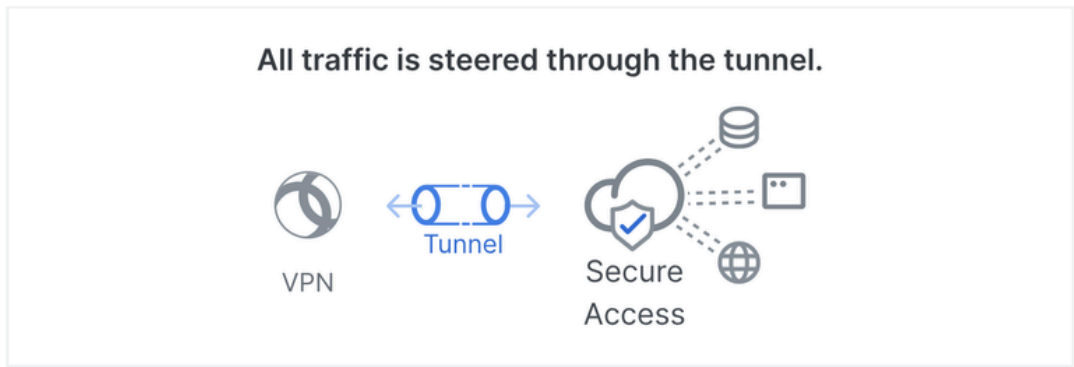
Tunnel Mode

Bypass Secure Access



- Si vous le souhaitez **Connect to Secure Access**, tous vos trafics Internet passent par **Secure Access**

Connect to Secure Access



Add Exceptions

Destinations specified here will be steered **OUTSIDE** the tunnel.

+ Add

Destinations	Exclude Destinations	Actions
proxy-8195126.zpc.sse.cisco.com, ztna.sse.cisco.com,acme.sse.cisco.com,devices.api.umbrella.com,sseposture-routing-commercial.k8s.5c10.org,sseposture-routing-commercial.posture.duosecurity.com,data.eb.thousandeyes.	-	-

Cancel

Back

Next

Si vous souhaitez ajouter des exclusions pour les domaines Internet ou les adresses IP, cliquez sur le + **Add** bouton, puis cliquez sur **Next**.

- Si vous le souhaitez **Bypass Secure Access**, tout votre trafic Internet passe par votre fournisseur d'accès Internet, et non par Secure Access (Pas de protection Internet)

Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

[+ Add](#)

Destinations

Exclude Destinations

Actions



No matches found

[Cancel](#)

[Back](#)

[Next](#)



Remarque : veuillez ajouter **enroll.cisco.com** pour la position ISE lorsque vous choisissez **Bypass Secure Access**.

Au cours de cette étape, vous sélectionnez toutes les ressources réseau privées auxquelles vous souhaitez accéder via le VPN. Pour ce faire, cliquez sur + **Add**, puis cliquez sur **Next** lorsque vous avez ajouté toutes les ressources.

Configuration du client sécurisé Cisco

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

Banner Message
Require user to accept a banner message post authentication

Session Timeout
 days

Session Timeout Alert
 minutes before

Maximum Transmission Unit ⓘ

[Cancel](#) [Back](#) [Save](#)

Dans cette étape, vous pouvez tout conserver par défaut et cliquer sur **Save**, mais si vous souhaitez personnaliser davantage votre configuration, consultez le [Guide de l'administrateur du client sécurisé Cisco](#).

Configurations ISE

Configurer la liste des périphériques réseau


Pour configurer l'authentification via Cisco ISE, vous devez configurer les périphériques autorisés qui peuvent émettre des requêtes vers votre Cisco ISE :

- Naviguez jusqu'à **Administration > Network Devices**
- Cliquez sur + **Add**

Network Devices

Name CSA

Description _____

IP Address * IP : 192.168.60.0 / 24 


Device Profile  Cisco 

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

Use Second Shared Secret 

Second Shared Secret _____ [Show](#)

CoA Port 1700 [Set To Default](#)

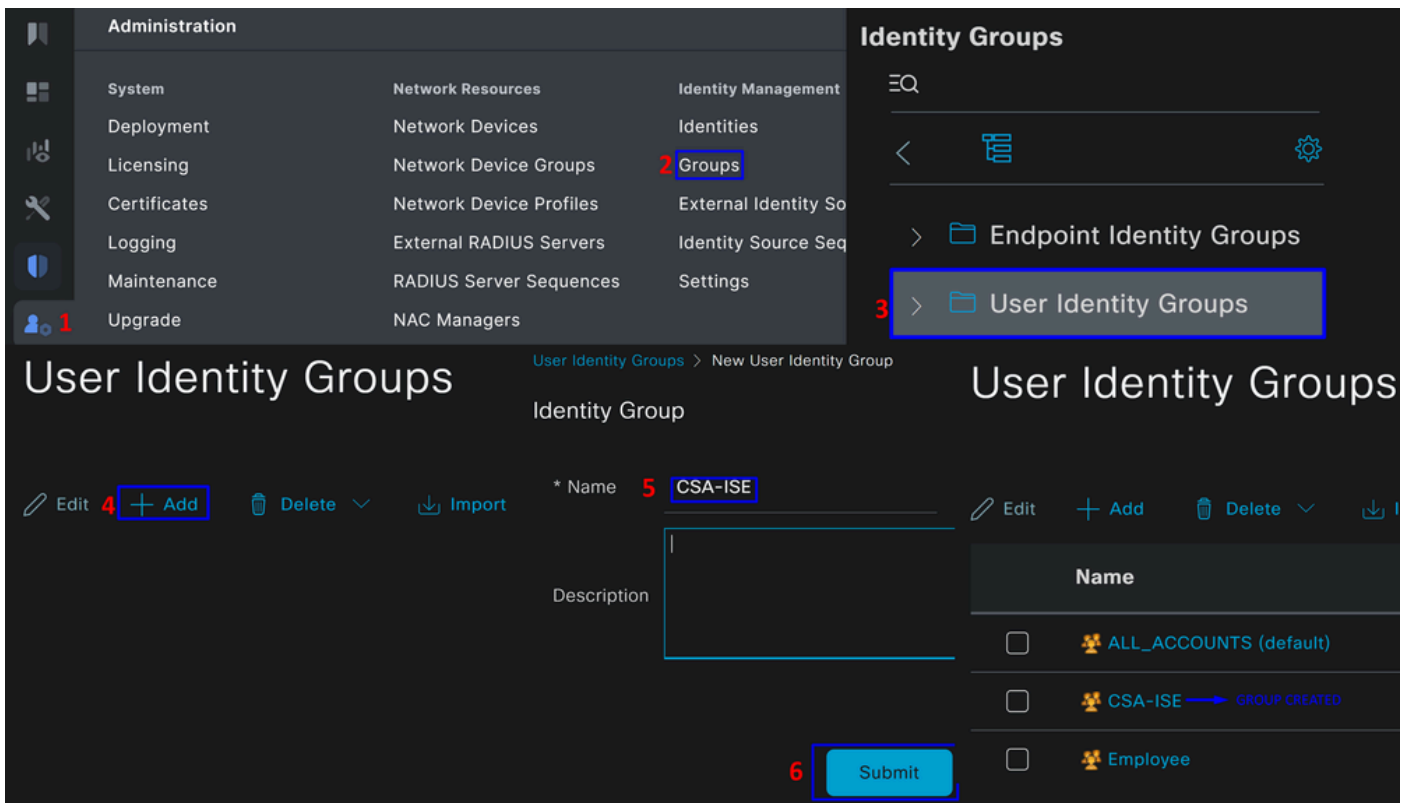
- **Name:** utilisez un nom pour identifier l'accès sécurisé
- **IP Address:** configurez le nom Management Interface de l'étape, [IP Pool Region](#)
- **Device Profile:** choisissez Cisco
 - **Radius Authentication Settings**
 - Shared Secret: Configurez le même secret partagé configuré à l'étape, [Clé secrète](#)
 - **CoA Port:** Laissez-le par défaut ; 1700 est également utilisé dans Secure Access

Après ce clic **Save**, pour vérifier si l'intégration fonctionne correctement, créez un utilisateur local pour la vérification de l'intégration.

Configurer un groupe

Pour configurer un groupe à utiliser avec des utilisateurs locaux, procédez comme suit :

- Cliquez dans **Administration > Groups**
- Cliquer **User Identity Groups**
- Cliquer + Add
- Créez un Name pour le groupe et cliquez sur **Submit**



Configurer l'utilisateur local

Pour configurer un utilisateur local afin de vérifier votre intégration :

- Naviguez jusqu'à **Administration > Identities**
- Cliquez sur **Add +**

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

	Password	Re-Enter Password	
* Login	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ
Enable	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ

▼ User Groups

⋮ ▼ 🗑️ +

- **Username:** Configurez le nom d'utilisateur avec un approvisionnement UPN connu dans Secure Access ; cela est basé sur l'étape, [Prérequis](#)
- **Status:** Actif
- **Password Lifetime:** Vous pouvez le configurer **With Expiration** ou Never Expires, selon vos besoins
- **Login Password:** crée un mot de passe pour l'utilisateur
- **User Groups:** sélectionnez le groupe créé à l'étape [Configurer un groupe](#)



Remarque : l'authentification basée sur UPN est configurée pour changer dans les prochaines versions de Secure Access.

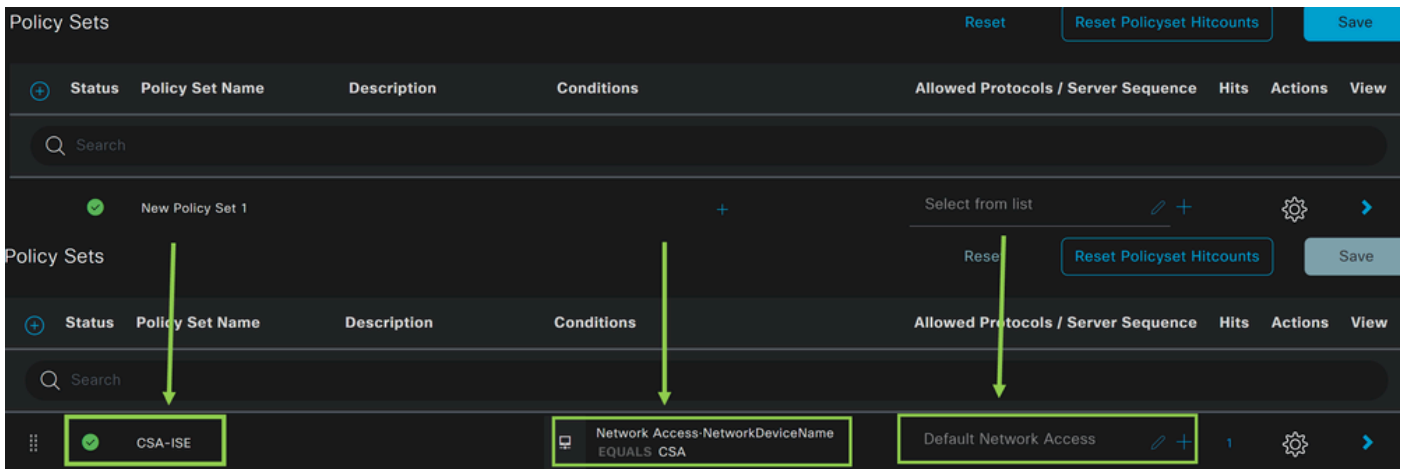
Après cela, vous pouvez **Save** modifier la configuration et passer à l'étape, **Configure Policy Set**.

Configurer le jeu de stratégies

Dans l'ensemble de stratégies, configurez l'action qu'ISE effectue pendant l'authentification et l'autorisation. Ce scénario illustre l'exemple d'utilisation de la configuration d'une stratégie simple pour fournir un accès utilisateur. Tout d'abord, ISE vérifie l'origine des authentifications RADIUS et vérifie si les identités existent dans la base de données utilisateur ISE pour fournir l'accès

Pour configurer cette stratégie, accédez à votre tableau de bord Cisco ISE :

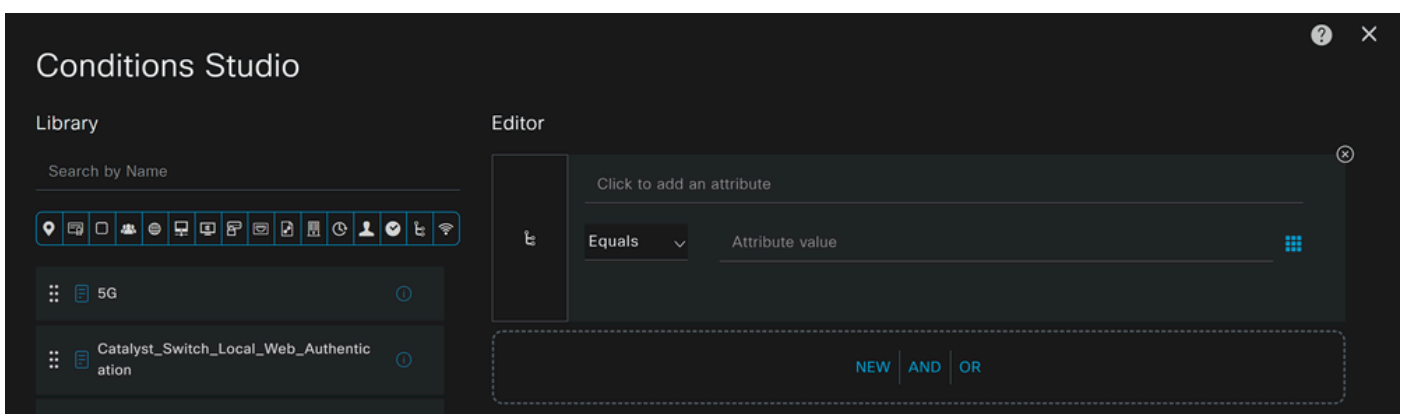
- Cliquez sur Policy > Policy Sets
- Cliquez sur + pour ajouter un nouvel ensemble de stratégies



Dans ce cas, créez un nouvel ensemble de stratégies au lieu de travailler avec celui par défaut. Configurez ensuite l'authentification et l'autorisation en fonction de cet ensemble de stratégies. La stratégie configurée autorise l'accès au périphérique réseau défini à l'étape [Configurer la liste des périphériques réseau](#) pour vérifier que ces authentifications proviennent de CSA Network Device List puis entrent dans la stratégie en tant que **Conditions**. Et enfin, les protocoles autorisés, comme **Default Network Access**.

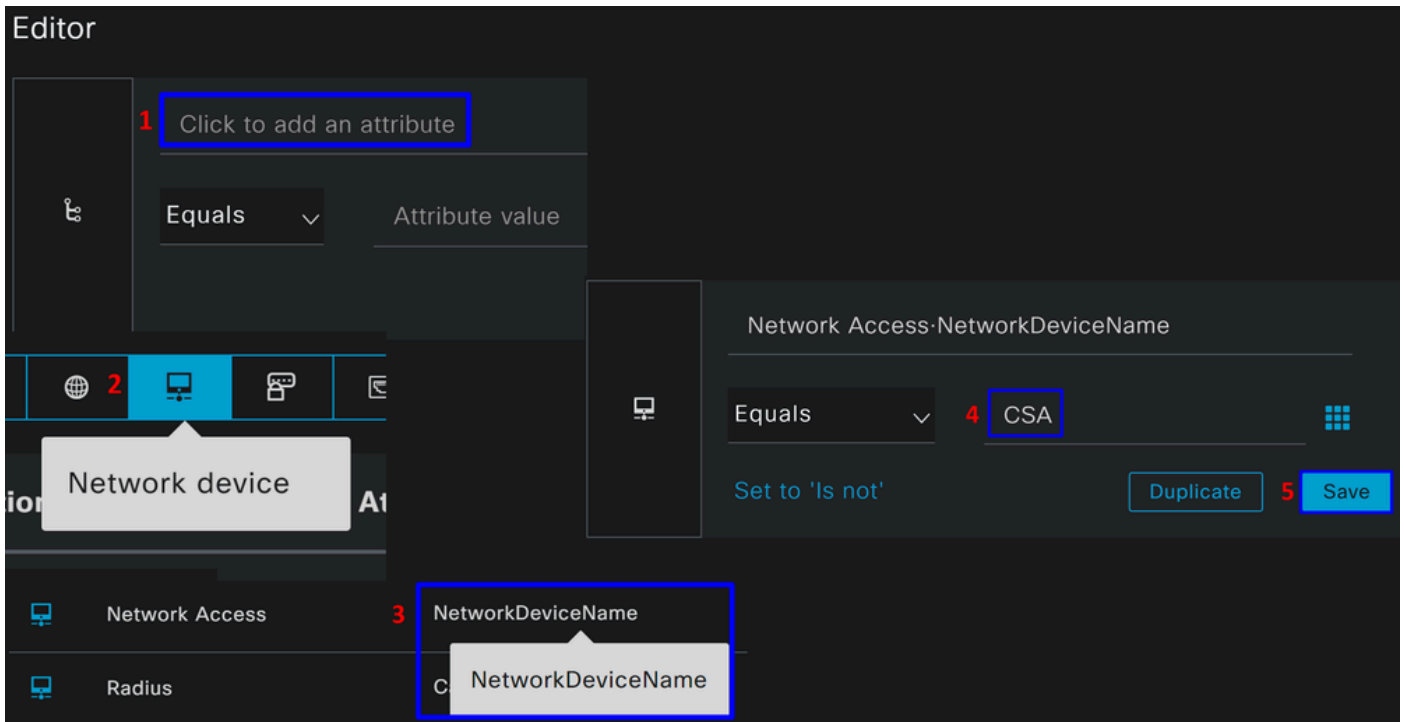
Pour créer le **condition** qui correspond au jeu de stratégies, procédez comme suit :

- Cliquez sur +
- Sous **Condition Studio**, les informations disponibles incluent :



- Pour créer les conditions, cliquez sur Click to add an attribute
- Cliquez sur le **Network Device** bouton
- Sous les options derrière, cliquez sur **Network Access - Network Device Name** option
- Sous l'option Equals, écrivez le nom du **Network Device** sous l'étape [Configure Network Devices List](#)

- Cliquer **Save**



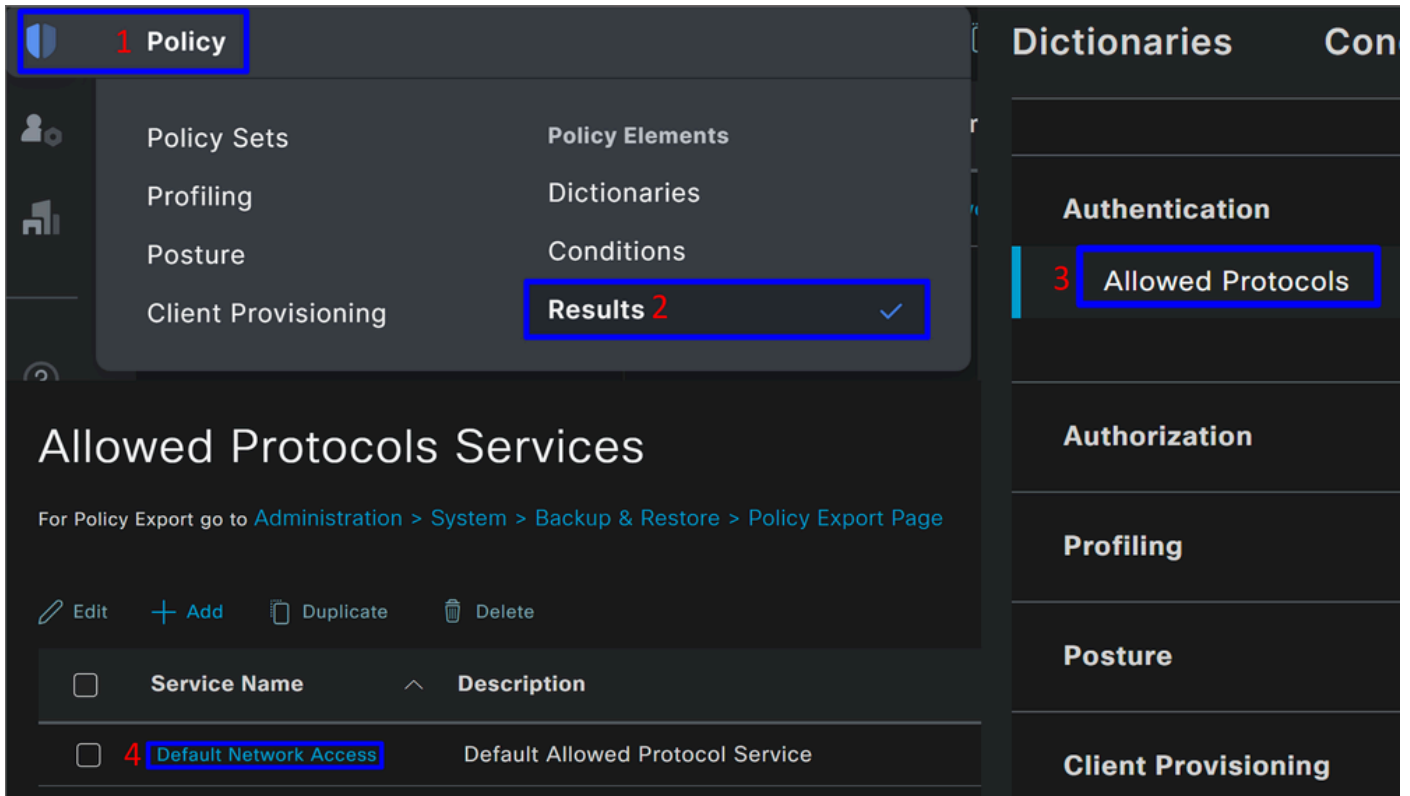
Cette stratégie approuve uniquement la demande de la source CSA de poursuivre l' **Authentication** et l' **Authorization** installation dans le cadre de l' ensemble de stratégies **CSA-ISE**, et vérifie également les protocoles autorisés en fonction de l' **Default Network Access** utilisation des protocoles autorisés.

Le résultat de la stratégie définie doit être :

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	CSA-ISE		Network Access·NetworkDeviceName EQUALS CSA	Default Network Access

- Pour vérifier les **Default Network Access Protocols** autorisations, procédez comme suit :

- Cliquez sur **Policy > Results**
 - Cliquez sur **Allowed Protocols**
 - Cliquez sur **Default Network Access**

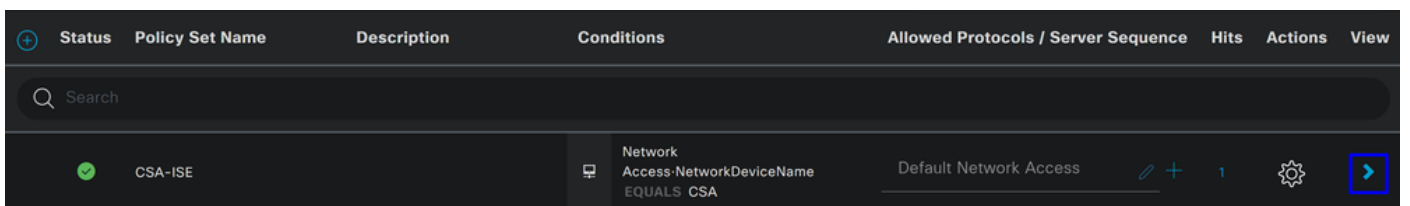


- Ensuite, vous voyez tous les protocoles autorisés sur **Default Network Access**

Configurer l'authentification et l'autorisation du jeu de stratégies

Pour créer la **Authentication** et la **Authorization** stratégie sous la **Policy Set**, procédez comme suit :

- Cliquez sur >



- Ensuite, les **Authentication** et les **Authorization** stratégies s'affichent :

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
🟢	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access
> Authentication Policy(2)				
> Authorization Policy - Local Exceptions				
> Authorization Policy - Global Exceptions				
> Authorization Policy(2)				

Stratégie d'authentification

Pour la stratégie d'authentification, vous pouvez configurer de nombreuses manières. Dans ce cas, vous voyez une politique pour le périphérique défini dans l'étape [Configurer la liste des périphériques réseau](#), et vérifiez l'authentification basée sur des critères spécifiques :

- Les utilisateurs authentifiés via le **Network Device CSA** ont réussi ou refusé l'authentification.

Authentication Policy(2)			
+ Status	Rule Name	Conditions	Use
🟢	Authentication Secure Access	Network Access:NetworkDeviceName EQUALS CSA	Internal Users
> Options			

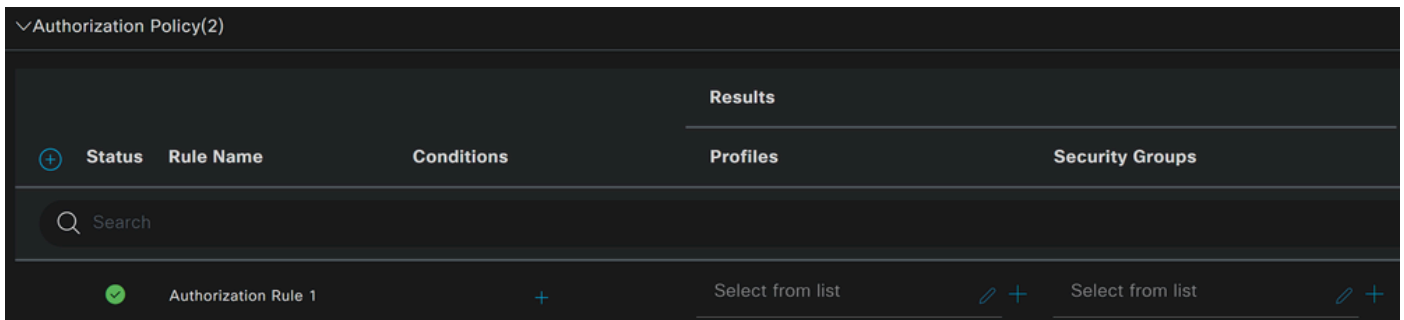
La stratégie est la même que celle définie à l'étape [Configure Policy Set](#).

Politique d'autorisation

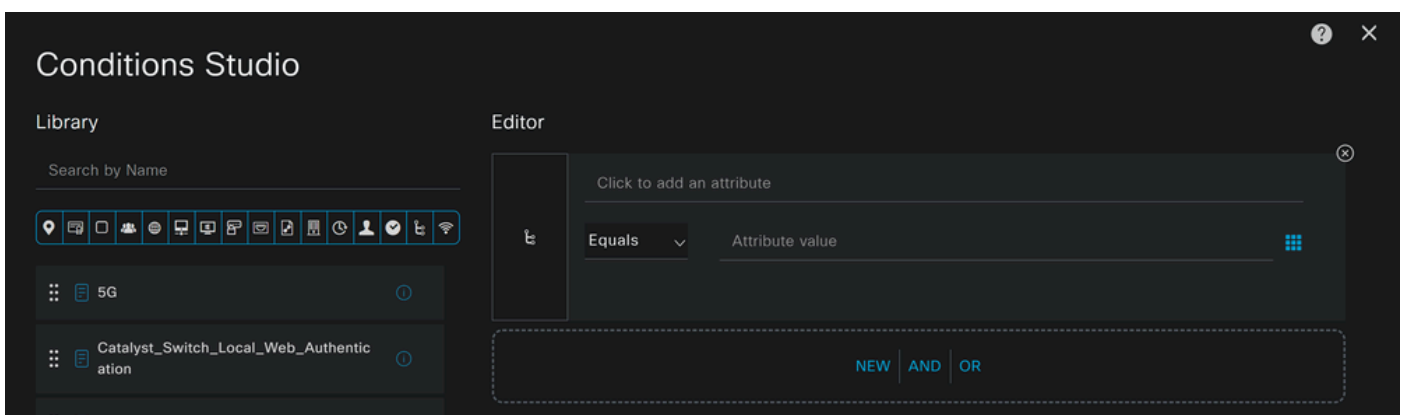
Vous pouvez configurer la stratégie d'autorisation de différentes manières. Dans ce cas, autorisez uniquement les utilisateurs du groupe défini à l'étape [Configurer un groupe](#). Consultez l'exemple suivant pour configurer votre stratégie d'autorisation :

Authorization Policy(2)				Results
+ Status	Rule Name	Conditions	Profiles	Security Groups
🟢	Authorization Rule 1		Select from list	Select from list
> Options				
🟢	Authorization Secure Access	InternalUser:IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list

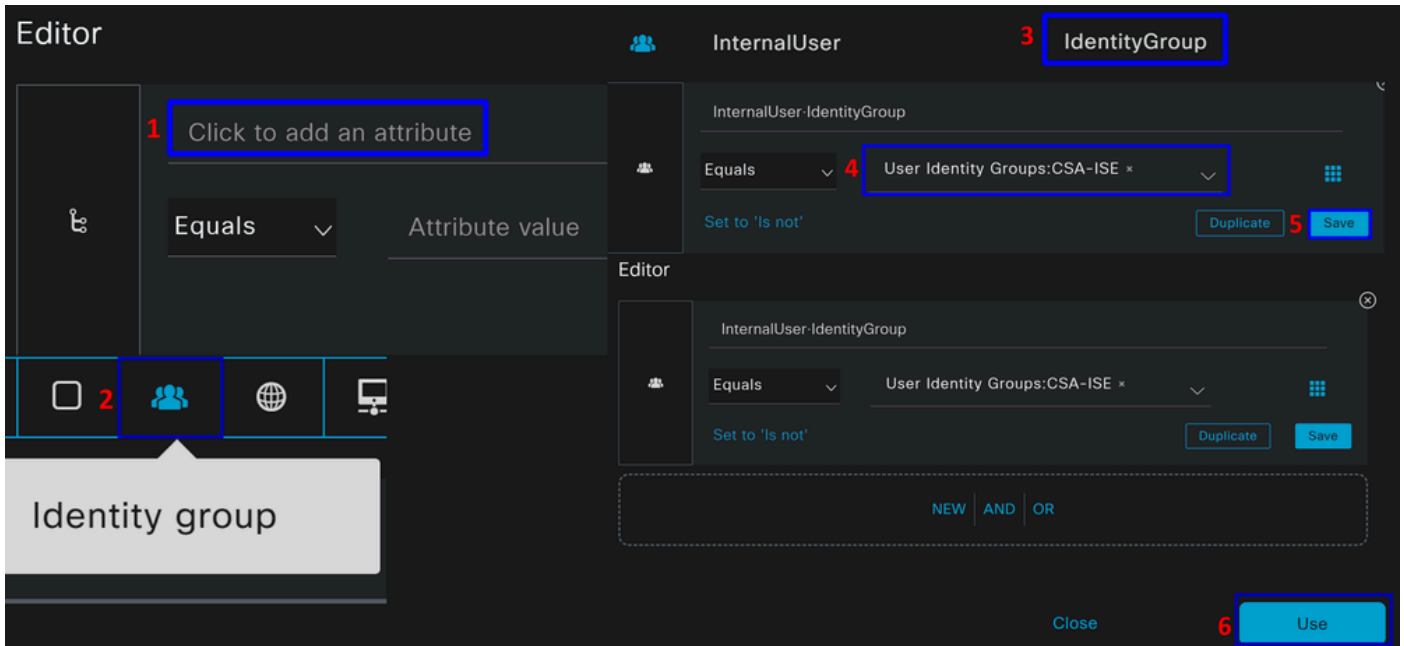
- Cliquez sur **Authorization Policy**
- Cliquez sur + pour définir la politique d'autorisation comme suit :



- Pour l'étape suivante, modifiez les Rule Name, Conditions et Profiles
- Lors de la définition de la **Name** configuration d'un nom pour identifier facilement la stratégie d'autorisation
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :



- Pour créer les conditions, cliquez sur Click to add an attribute
- Cliquez sur le **Identity Group** bouton
- Sous les options derrière, cliquez sur **Internal User - IdentityGroup** option
- Sous l'**Equals** option, utilisez la liste déroulante pour rechercher le **Group** approuvé pour l'authentification à l'étape, [Configurer un groupe](#)
- Cliquer **Save**
- Cliquer **Use**



Après cela, vous devez définir le **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Sous le **Authorization Policy**, cliquez sur le bouton déroulant sur **Profiles**
- Rechercher un permis
- Sélectionner **PermitAccess**
- Cliquer Save

InternalUser-IdentityGroup
EQUALS User Identity
Groups:CSA-ISE

Select from list

InternalUser-IdentityGroup
EQUALS User Identity
Groups:CSA-ISE

2 permit

Profiles

3 PermitAccess

IdentityGroup
Identity

PermitAccess x

Select from list

DenyAccess

Select from list

Reset 4 Save

Après cela, vous avez défini votre stratégie **Authentication Authorization** et. Authentifiez-vous pour vérifier si l'utilisateur se connecte sans problème et si vous pouvez voir les journaux sur Secure Access et ISE.

Pour vous connecter au VPN, vous pouvez utiliser le profil créé sur Secure Access et vous connecter via Secure Client avec le profil ISE.

- **Comment le journal s'affiche-t-il dans Secure Access lorsque l'authentification est approuvée ?**

- Accédez au tableau de bord [Secure Access](#)
- Cliquez sur **Monitor > Remote Access Log**

28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
vpn user (vpnuser@ciscosst.es)	Connected		192.168.50.2	151.248.21.152	ISE_CSA

- **Comment le journal s'affiche-t-il dans ISE lorsque l'authentification est approuvée ?**

- Accédez à la page **Cisco ISE Dashboard**

- Cliquez sur **Operations > Live Logs**

Status	Details	Identity	Authentication Policy	Authorization Policy
✕	∨	Identity	Authentication Policy	Authorization Policy
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access

Configuration des utilisateurs de Radius Local ou Active Directory

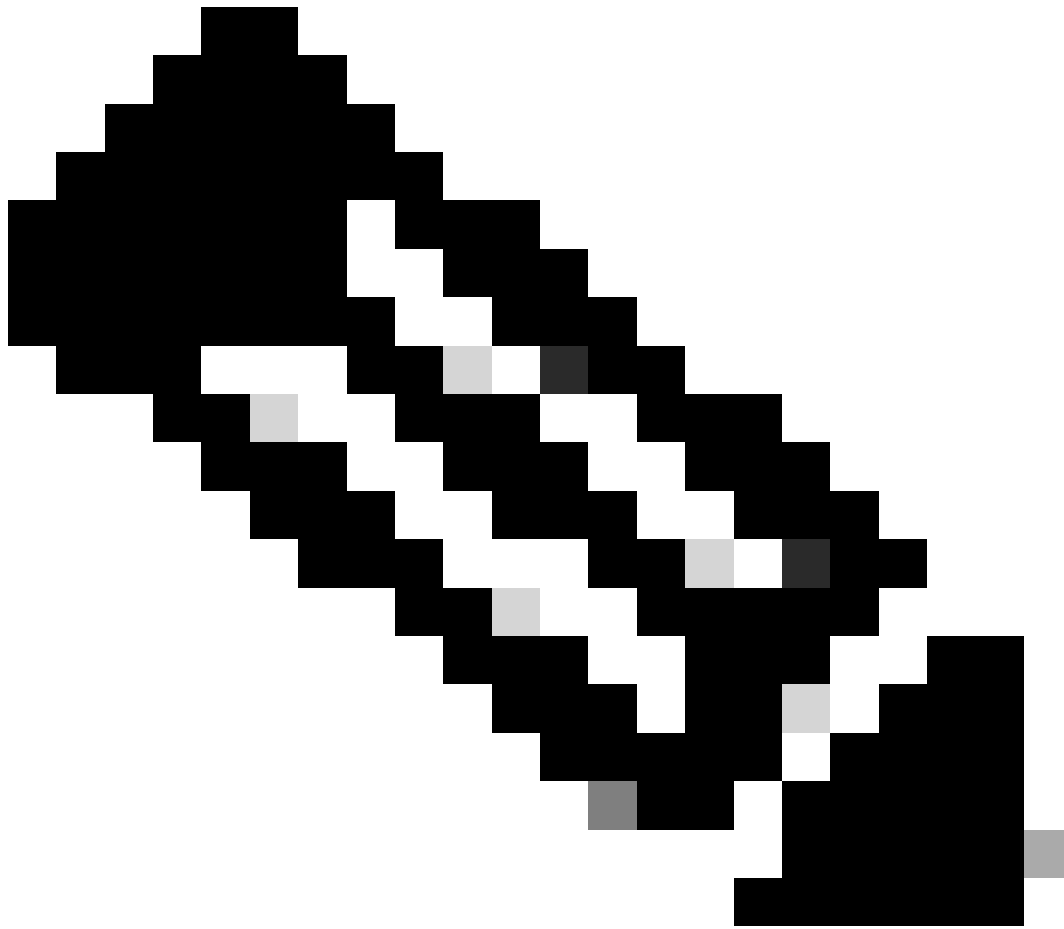
Configuration de la position ISE

Dans ce scénario, créez la configuration pour vérifier la conformité des terminaux avant d'accorder ou de refuser l'accès aux ressources internes.

Pour le configurer, passez aux étapes suivantes :

Configuration des conditions de posture

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center > Policy Elements > Conditions**
- Cliquez sur **Anti-Malware**



Remarque : vous y trouverez de nombreuses options pour vérifier la position de vos périphériques et effectuer l'évaluation correcte en fonction de vos politiques internes.

Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource

File

Firewall

Anti-Malware Condition pour détecter l'installation de l'antivirus sur le système ; vous pouvez également choisir la version du système d'exploitation si nécessaire.

The image shows two side-by-side screenshots of the 'Anti-Malware Condition' configuration interface. The left screenshot shows a form with the following fields: '* Name' (empty), 'Description' (empty), 'Compliance Module' (4.x or later), '* Operating System' (Select Operating System), and 'Vendor' (ANY). The 'Check Type' is set to 'Installation'. The right screenshot shows the same form with the following values: '* Name' (CSA-Antimalware), 'Description' (empty), 'Compliance Module' (4.x or later), '* Operating System' (Windows All), and 'Vendor' (Cisco Systems, Inc.). The 'Check Type' is also set to 'Installation'. Arrows point from the left form to the right form, indicating a transition or comparison of values.

- **Name:** utilisez un nom pour reconnaître la condition anti-programme malveillant
- **Operating System:** choisissez le système d'exploitation que vous souhaitez mettre sous la condition
- **Vendor:** choisissez un fournisseur ou ANY
- **Check Type:** vous pouvez vérifier si l'agent est installé ou la version de définition de cette option.
- Pour **Products for Selected Vendor**, vous configurez ce que vous souhaitez vérifier à propos du logiciel anti-programme malveillant sur le périphérique.

Baseline Condition Advanced Condition

1 You can select products either on baseline condition or advanced condition.

2

	Product Name	Minimum Version	Maximum Version	Minimum Compliant
<input type="checkbox"/>	ANY	ANY	ANY	N/A
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.2.520.0
<input checked="" type="checkbox"/>	Cisco Advanced Malware Prote...	5.x	7.x	4.3.2815.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint	7.x	8.x	4.3.3726.6145
<input checked="" type="checkbox"/>	Cisco Secure Endpoint (x86)	7.x	8.x	4.3.3726.6145
<input type="checkbox"/>	ClamAV	0.x	ClamAV0.x	4.3.2868.6145

3

Save Reset

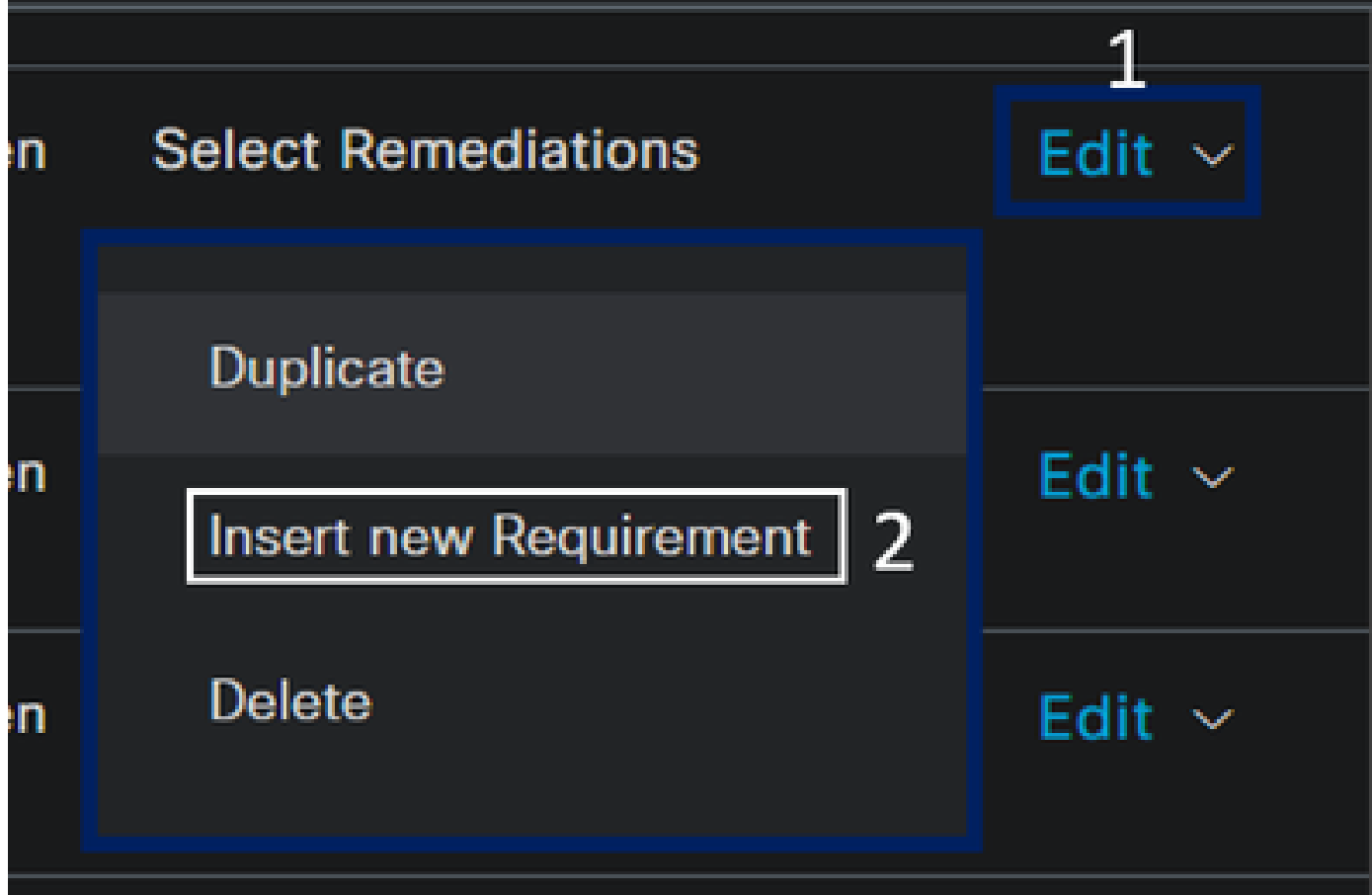
- Cochez la case correspondant aux conditions que vous souhaitez évaluer
- Configurez la version minimale à vérifier
- Cliquez sur Enregistrer pour passer à l'étape suivante

Une fois que vous l'avez configuré, vous pouvez passer à l'étape **Configure Posture Requirements**.

Configuration des exigences de posture

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center > Policy Elements > Requiriments**
- Cliquez sur **Edit** l'une des conditions requises, puis sur **Insert new Requirement**

Remediations Actions



- Sous la nouvelle condition, configurez les paramètres suivants :

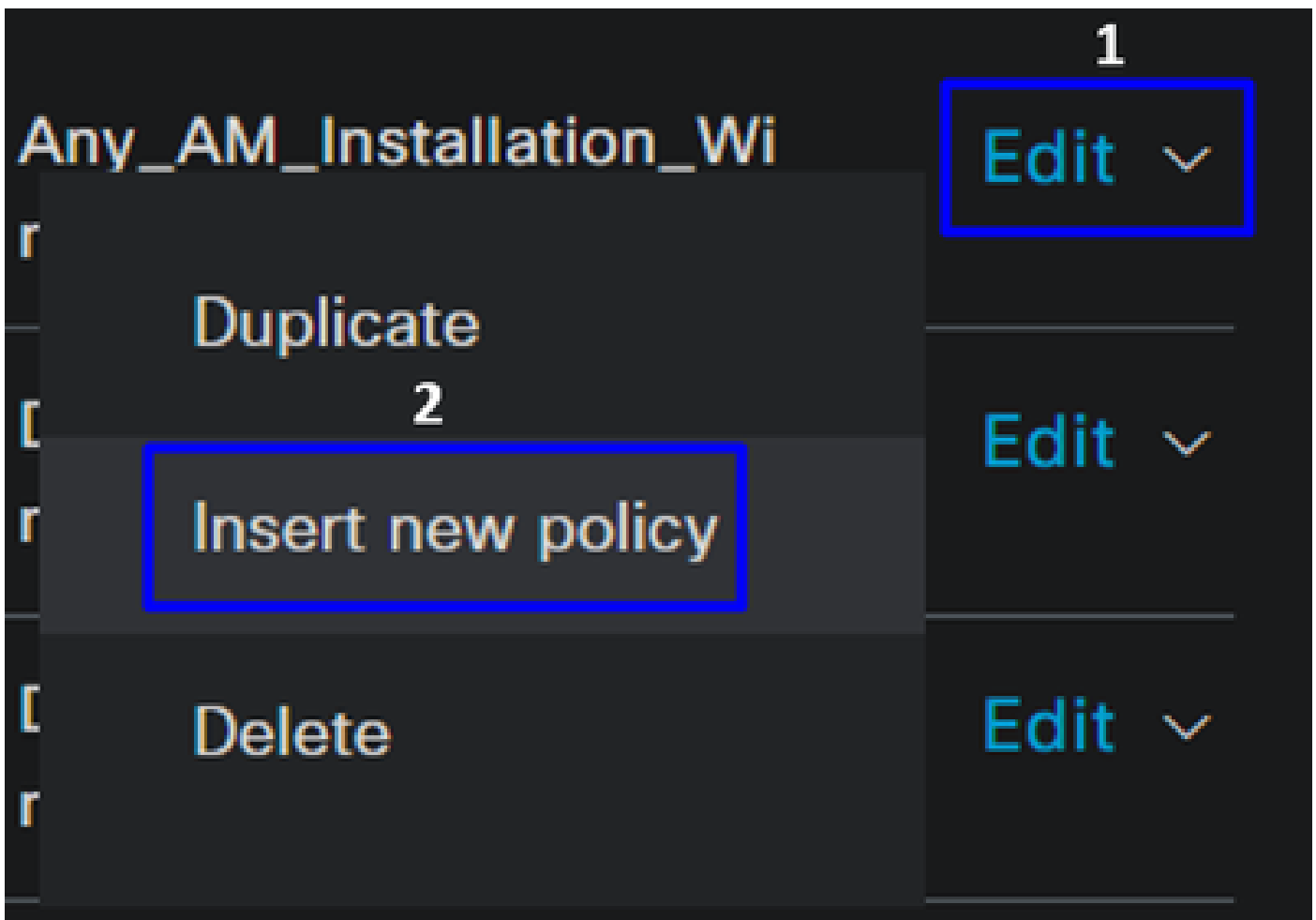
Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
CSA-ANTIMALWARE	for Windows All	using 4.x or later	using Agent	met if CSA-Antimalware then	Message Text Only

- **Name:** configurez un nom pour reconnaître la condition requise en matière de protection contre les programmes malveillants
- **Operating System:** choisissez le système d'exploitation que vous choisissez dans l'étape de condition, [Système d'exploitation](#)
- **Compliance Module:** Vous devez vous assurer de sélectionner le même module de conformité que celui que vous avez sous l'étape de condition, [Condition anti-programme malveillant](#)
- **Posture Type:** Choisir un agent
- **Conditions:** sélectionnez la ou les conditions que vous avez créées à l'étape [Configurer les conditions de posture](#)
- **Remediations Actions:** choisissez **Message Text Only** pour cet exemple ou, si vous disposez d'une autre action corrective, utilisez-la
- Cliquer **Save**

Une fois la configuration effectuée, vous pouvez passer à l'étape suivante : **Configure Posture Policy**

Configurer la politique de posture

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center > Posture Policy**
- Cliquez sur **Edit** l'une des stratégies, puis sur **Insert new Policy**



- Dans la nouvelle stratégie, configurez les paramètres suivants :

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	CSA-Windows-Posture	If Any	and Windows All	and 4.x or later	and Agent	and	then CSA-ANTIMALWARE

- **Status:** cochez la case no enable the policy
- **Rule Name:** configurez un nom pour reconnaître la stratégie configurée

- **Identity Groups:** choisissez les identités que vous souhaitez évaluer
- **Operating Systems:** choisissez le système d'exploitation en fonction de la condition et de la condition configurées avant
- **Compliance Module:** choisissez le module de conformité en fonction de la condition et de la condition configurées avant
- Posture Type: Choisir un agent
- **Requirements:** choisissez les exigences configurées à l'étape [Configurer les exigences de posture](#)
- Cliquer **Save**

Configurer le provisionnement client

Pour fournir aux utilisateurs le module ISE, configurez le provisionnement client pour équiper les machines du module de posture ISE. Cela vous permet de vérifier la position des machines une fois l'agent installé. Pour poursuivre ce processus, voici les étapes suivantes :

Accédez à votre tableau de bord ISE.










- Cliquez sur **Work Center > Client Provisioning**
- Choisir **Resources**

Vous devez configurer trois éléments dans le cadre du provisionnement du client :

Ressources à configurer	Description
1. Agent Resources	Package d'approvisionnement Web du client sécurisé.
2. Compliance Module	Module de conformité Cisco ISE
3. Agent Profile	Contrôle du profil d'approvisionnement.
3. Agent Configuration	Définissez les modules à provisionner en configurant le portail de provisionnement, à l'aide du profil d'agent et des ressources d'agent.

Step 1 Télécharger et charger les ressources de l'agent

- Pour ajouter une nouvelle ressource d'agent, accédez au [portail de téléchargement Cisco](#) et téléchargez le package de déploiement Web ; le fichier de déploiement Web doit être au format .pkg.

Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	58.06 MB	  
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB	  
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	118.88 MB	  

- Cliquez sur + Add > Agent resources from local disk et téléchargez les packages

+ Add ^ Duplicate Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

Step 2 Télécharger le module de conformité

- Cliquez sur + Add > Agent resources from Cisco Site

+ Add ^ Duplicate Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- Cochez la case correspondant à chaque module de conformité requis et cliquez sur **Save**

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Step 3 Configuration du profil d'agent

- Cliquez sur + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑 Delet

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- Créez un **Name** pour le **Posture Profile**

Agent Posture Profile

Name *



Description:

- Sous Règles de nom de serveur, placez un * et cliquez **Save** ensuite

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Step 4 Configuration de l'agent

- Cliquez sur + Add > Agent Configuration

+ Add ^

📱 Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- Ensuite, configurez les paramètres suivants :

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

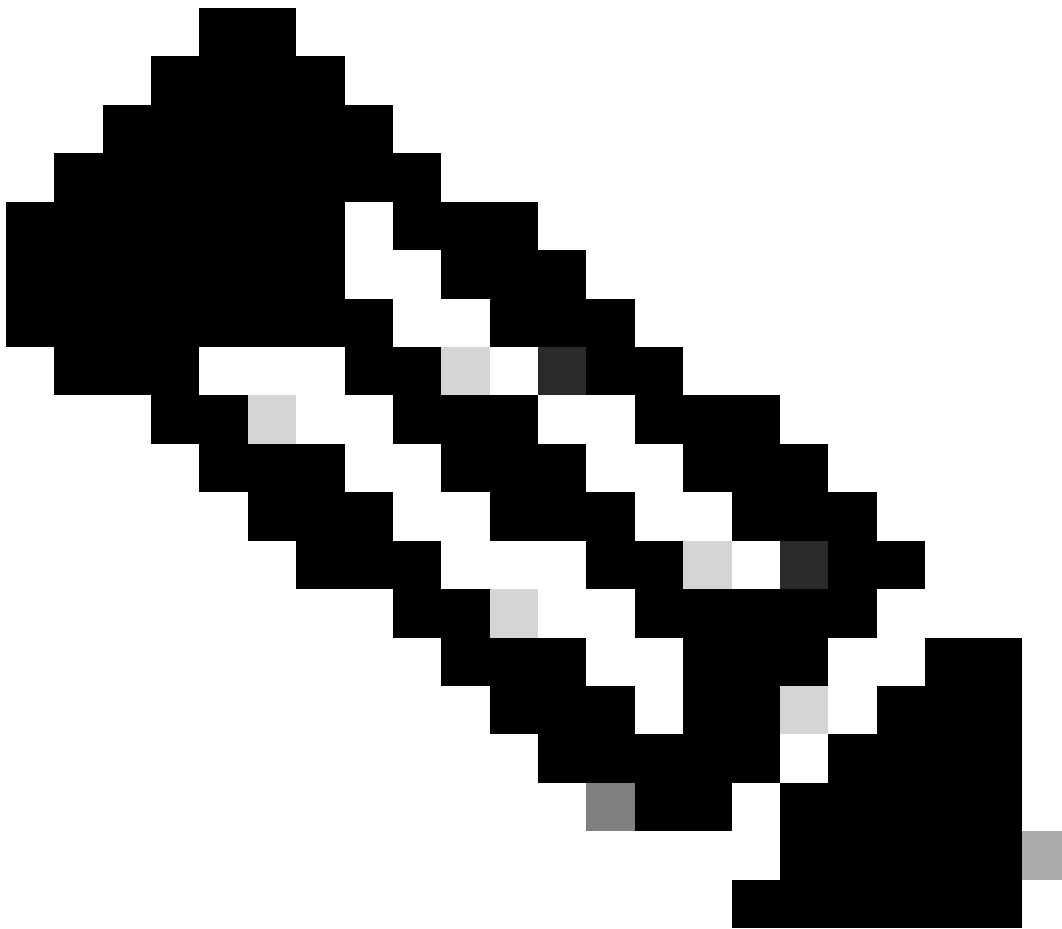
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- Select Agent Package : choisissez le package téléchargé dans les [ressources de l'agent de téléchargement et de téléchargement de l'étape 1](#)
- **Configuration Name:** choisissez un nom pour reconnaître le **Agent Configuration**
- **Compliance Module:** sélectionnez le module de conformité téléchargé à l'[étape 2 Télécharger le module de conformité](#)
- Cisco Secure Client Module Selection
 - **ISE Posture:** cochez la case
- **Profile Selection**

- **ISE Posture:** sélectionnez le profil ISE configuré à l'[étape 3 Configuration du profil d'agent](#)

- Cliquer **Save**
-

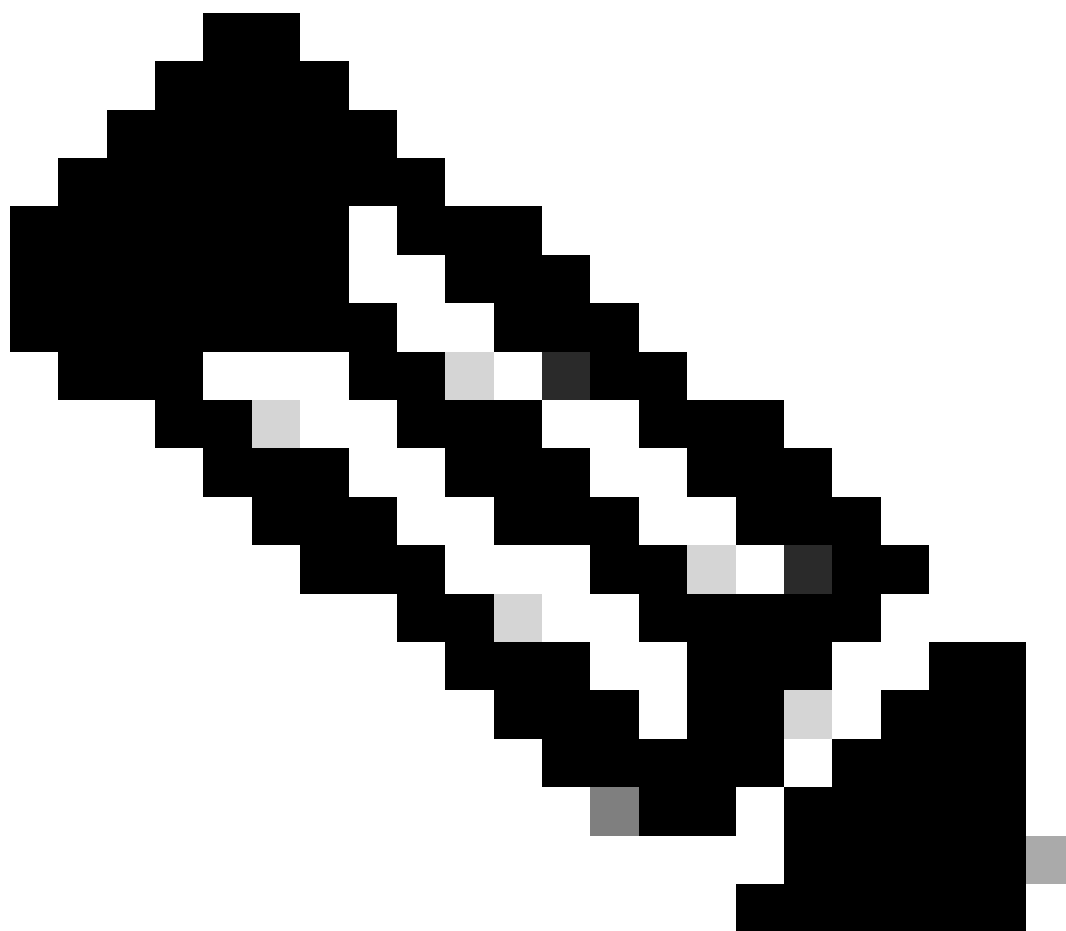


Remarque : il est recommandé que chaque système d'exploitation, Windows, Mac OS ou Linux, dispose d'une configuration client indépendante.

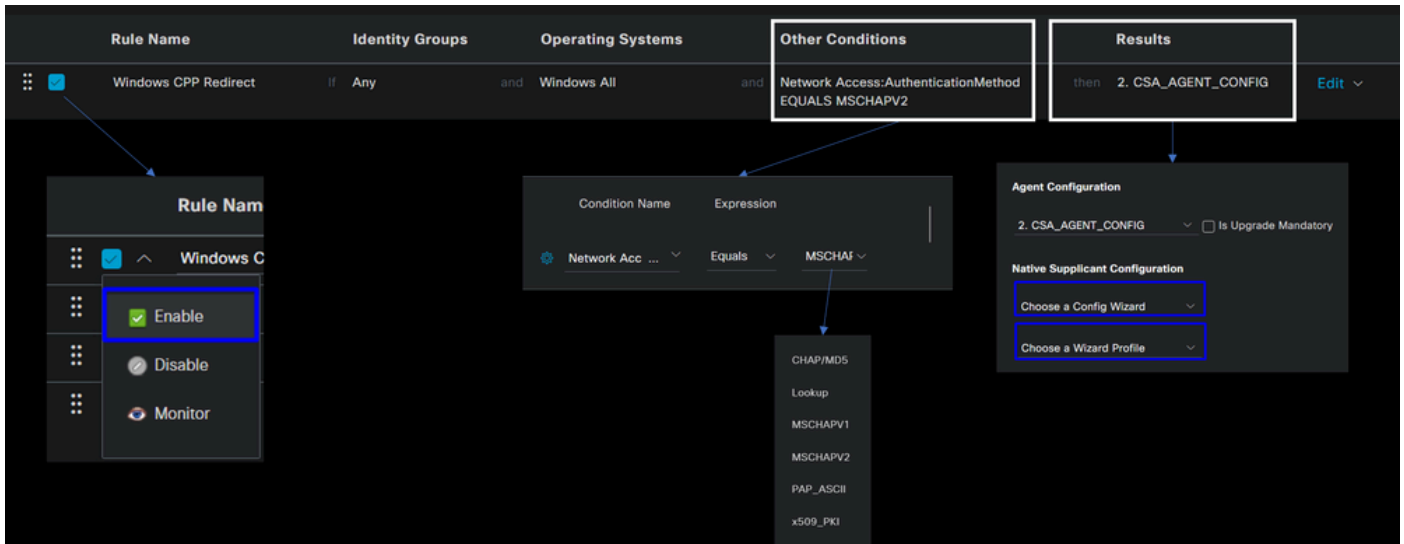
Configurer la politique de provisionnement client

Pour activer le provisionnement de la position ISE et des modules configurés à la dernière étape, vous devez configurer une stratégie pour effectuer le provisionnement.

- Accédez à votre tableau de bord ISE
- Cliquez sur **Work Center > Client Provisioning**



Remarque : il est recommandé que chaque système d'exploitation, Windows, Mac OS ou Linux, dispose d'une stratégie de configuration client.



- **Rule Name:** configurez le nom de la stratégie en fonction du type de périphérique et du groupe d'identités sélectionnés afin d'identifier facilement chaque stratégie
- **Identity Groups:** choisissez les identités que vous souhaitez évaluer sur la stratégie
- **Operating Systems:** choisissez le système d'exploitation en fonction du package d'agent sélectionné à l'étape [Sélectionner un package d'agent](#)
- **Other Condition:** choisissez en **Network Access** fonction de la méthode **Authentication Method** EQUALS configurée à l'étape, [Ajouter un groupe RADIUS](#) ou laissez en blanc
- **Result:** sélectionnez la configuration de l'agent configurée à l'[étape 4. Configurez la configuration de l'agent](#)
 - **Native Supplicant Configuration:** sélectionnez Config Wizard et Wizard Profile
- Marquez la stratégie comme étant activée si elle n'est pas répertoriée comme étant activée dans la case à cocher.

Créer les profils d'autorisation

Le profil d'autorisation limite l'accès aux ressources en fonction de la position des utilisateurs après le passage de l'authentification. L'autorisation doit être vérifiée pour déterminer les ressources auxquelles l'utilisateur peut accéder en fonction de la position.

Profil d'autorisation	Description
Conforme	Compatible utilisateur - Agent installé - Posture vérifiée
Conformité	User Unknown Compliant - Rediriger pour installer l'agent - Position en attente

inconnue	à vérifier
RefuserAccès	Utilisateur non conforme - Refuser l'accès

Pour configurer la liste de contrôle d'accès, accédez au tableau de bord ISE :

- Cliquez sur **Work Centers > Policy Elements > Downloadable ACLs**
- Cliquez sur **+Add**
- Créez le **Compliant DACL**

* Name: CSA-Compliant

Description: [Empty text box]

IP version: IPv4 IPv6 Agnostic ⓘ

* DACL Content:

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
0000000	

- **Name:** ajoutez un nom qui fait référence à la conformité DACL
- **IP version:** Choisir **IPv4**
- **DACL Content:** création d'une liste de contrôle d'accès téléchargeable (DACL) donnant accès à toutes les ressources du réseau

<#root>

permit ip any any

Cliquez sur **Save** et créez la DACL de conformité inconnue

- Cliquez sur **Work Centers > Policy Elements > Downloadable ACLs**

- Cliquez sur **+Add**
- Créez le **Unknown Compliant DACL**

*** Name**

Description

IP version IPv4 IPv6 Agnostic i

* DACL Content	
1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

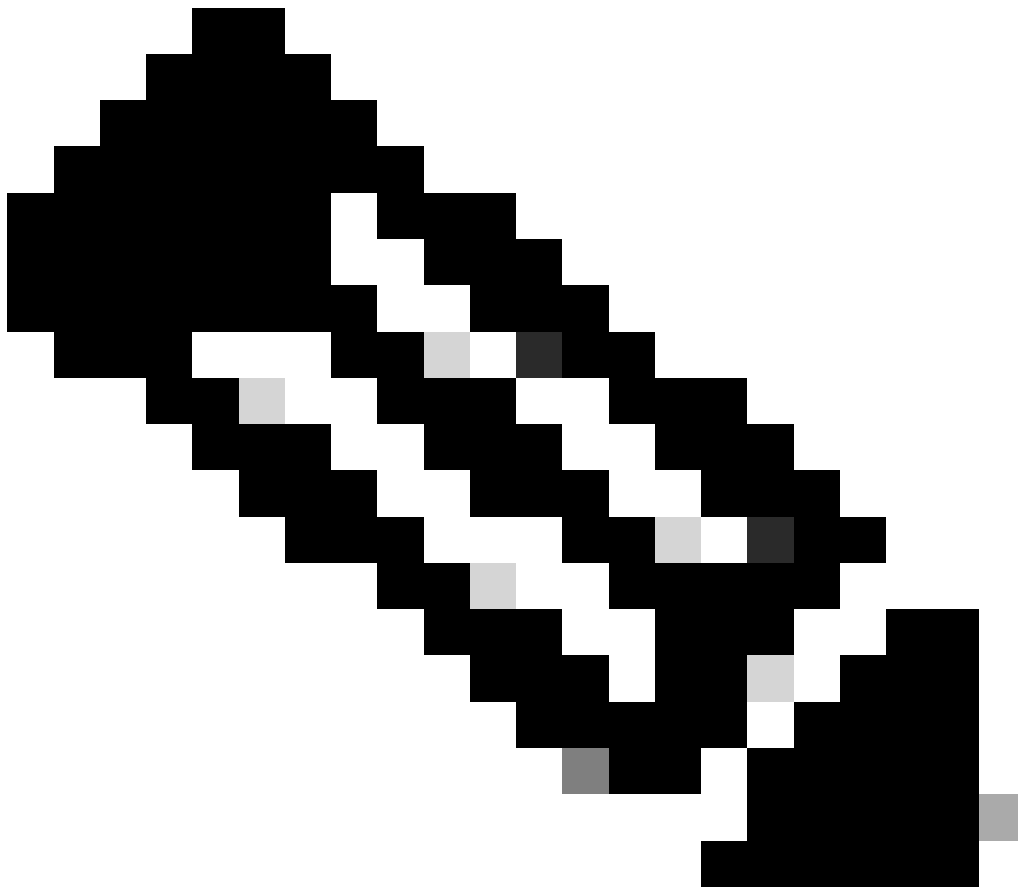
Check DACL Syntax

- **Name:** ajoutez un nom qui fait référence à la DACL-Unknown-Compliant
- **IP version:** Choisir **IPv4**
- **DACL Content:** Créez une liste de contrôle d'accès DACL qui donne un accès limité au réseau, DHCP, DNS, HTTP et au portail d'approvisionnement sur le port 8443

```

permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443

```

Remarque : dans ce scénario, l'adresse IP 192.168.10.206 correspond au serveur Cisco Identity Services Engine (ISE) et le port 8443 est désigné pour le portail de mise en service. Cela signifie que le trafic TCP vers l'adresse IP 192.168.10.206 via le port 8443 est autorisé, ce qui facilite l'accès au portail d'approvisionnement.

À ce stade, vous disposez de la liste de contrôle d'accès requise pour créer les profils d'autorisation.

Pour configurer les profils d'autorisation, accédez au tableau de bord ISE :

- Cliquez sur **Work Centers > Policy Elements > Authorization Profiles**

- Cliquez sur **+Add**

- Créez le **Compliant Authorization Profile**

Authorization Profile

* Name


CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

 Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

✓ Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL IPv6 (Filter ID)

- **Name:** créez un nom faisant référence au profil d'autorisation conforme
- Access Type: Choisir **ACCESS_ACCEPT**

- **Common Tasks**

- **DACL NAME:** sélectionnez la DACL configurée à l'étape [DACL conforme](#)

Cliquez sur **Save** et créez le Unknown Authorization Profile



- Cliquez sur **Work Centers > Policy Elements > Authorization Profiles**
- Cliquez sur **+Add**

- Créez le **Unknown Compliant Authorization Profile**


*** Name** CSA-Unknown-Compliant


Description


*** Access Type** ACCESS_ACCEPT ▼

Network Device Profile  Cisco ▼ 

Service Template

Track Movement 

Agentless Posture 

Passive Identity Tracking 

▼ **Common Tasks**

DACL Name CSA_Redirect_To_ISE ▼

Web Redirection (CWA, MDM, NSP, CPP) 

Client Provisioning (Posture) ▼ **ACL** **redirect** ▼ **Value** **Client Provisioning Portal (...)** ▼

- **Name:** créez un nom faisant référence au profil d'autorisation conforme inconnu
- Access Type: Choisir **ACCESS_ACCEPT**

- **Common Tasks**

- **DACL NAME:** sélectionnez la DACL configurée à l'étape [DACL conforme inconnu](#)

- **Web Redirection (CWA,MDM,NSP,CPP)**

- Choisir **Client Provisioning (Posture)**

- **ACL:** doit être redirect
 - **Value:** choisissez le portail de mise en service par défaut ou, si vous en avez défini un autre, choisissez-le
-
-

Remarque : le nom de la liste de contrôle d'accès de redirection sur l'accès sécurisé pour tous les déploiements est **redirect**.

Une fois que vous avez défini toutes ces valeurs, vous devez avoir quelque chose de similaire sous Attributes Details.

Attributes Details

Access Type = ACCESS_ACCEPT

DAACL = CSA_Redirect_To_ISE

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=

&action=cpp

Cliquez sur ce bouton **Save** pour mettre fin à la configuration et passer à l'étape suivante.

Configurer le jeu de stratégies de position

Ces trois stratégies que vous créez sont basées sur les profils d'autorisation que vous avez configurés ; par **DenyAcces** exemple, vous n'avez pas besoin d'en créer un autre.

Ensemble de stratégies - Autorisation	Profil d'autorisation
Conforme	Profil d'autorisation - Conforme
Conformité inconnue	Profil d'autorisation - Inconnu Conforme
Non Conforme	RefuserAccès

Accédez à votre tableau de bord ISE

- Cliquez sur **Work Center > Policy Sets**

- Cliquez sur > pour accéder à la stratégie que vous avez créée

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access	370		

- Cliquez sur le bouton Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
> Authorization Policy(4)					

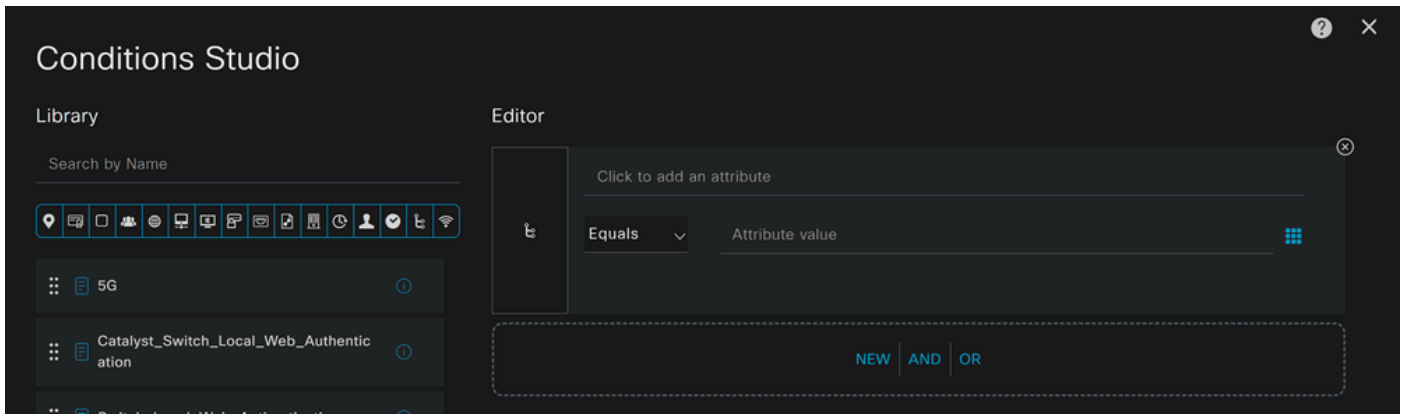
- Créez les trois stratégies suivantes dans l'ordre suivant :

✓	CSA-Compliant	AND	<ul style="list-style-type: none"> Compliant_Devices Network_Access_Authentication_Passed InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	CSA-Post-Compliant
✓	CSA-Unknown-Compliant	AND	<ul style="list-style-type: none"> Network_Access_Authentication_Passed Compliance_Unknown_Devices InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	CSA-Unknown-Compliant
✓	CSA-Non-Compliant	AND	<ul style="list-style-type: none"> Non_Compliant_Devices Network_Access_Authentication_Passed InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	DenyAccess

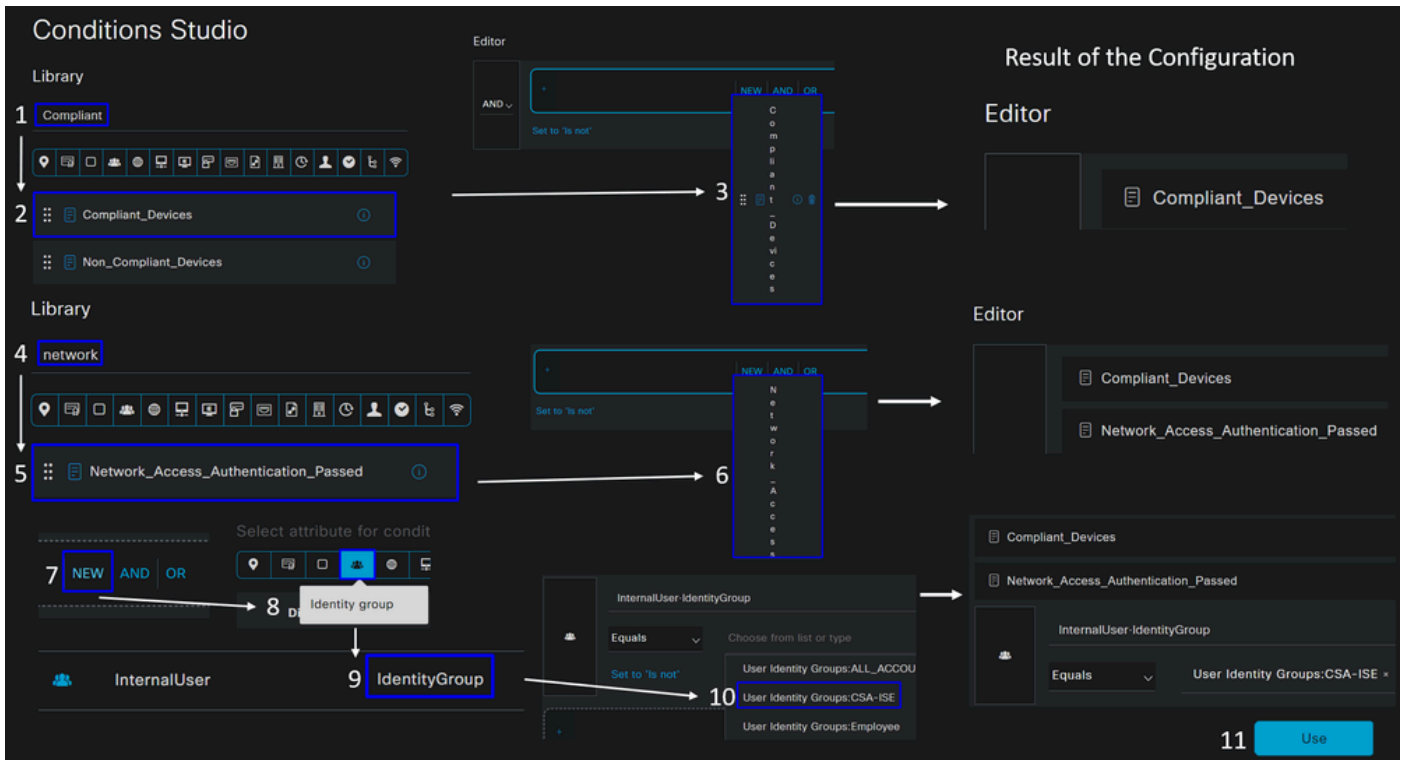
- Cliquez sur + pour définir la **CSA-Compliance** politique :

				Results	
+ Status	Rule Name	Conditions		Profiles	Security Groups
Search					
✓	Authorization Rule 1	+		Select from list	Select from list

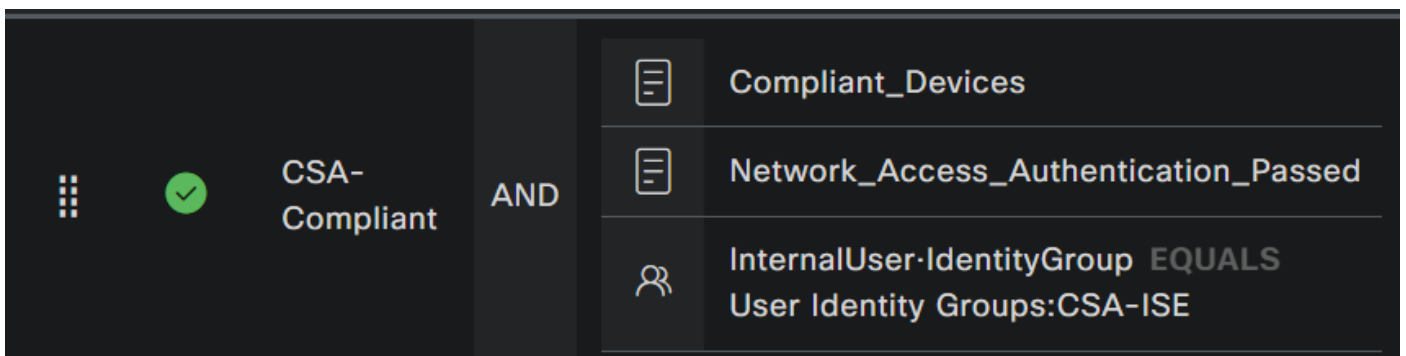
- Pour l'étape suivante, modifiez les Rule Name, Conditions et Profiles
- Lorsque vous définissez le paramètre **Name** configure a name sur **CSA-Compliance**
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :



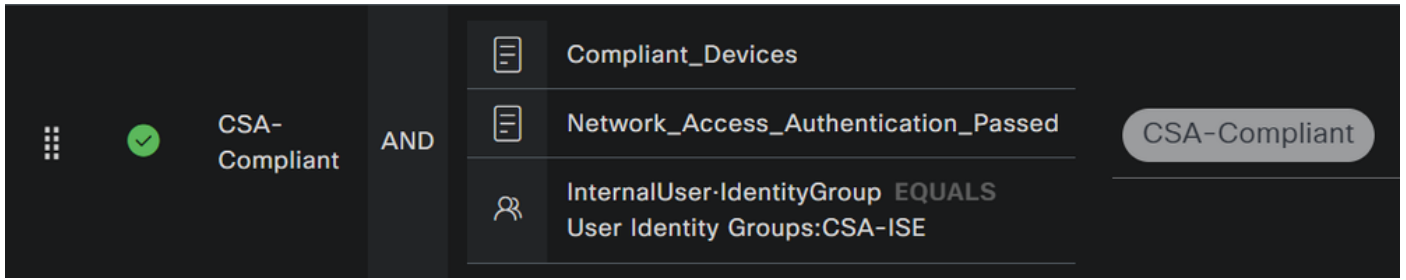
- Pour créer la condition, recherchez **compliant**
- Vous devez avoir affiché Compliant_Devices
- Glisser-déplacer sous le **Editor**
- Pour créer la deuxième condition, recherchez **network**
- Vous devez avoir affiché Network_Access_Authentication_Passed
- Glisser-déplacer sous le **Editor**
- Cliquez sous la Editor dans **New**
- Cliquez sur l'**Identity Group** icône
- Choisir **Internal User Identity Group**
- Sous **Equals**, sélectionnez le **User Identity Group** que vous souhaitez faire correspondre
- Cliquer **Use**



- Par conséquent, vous obtenez l'image suivante

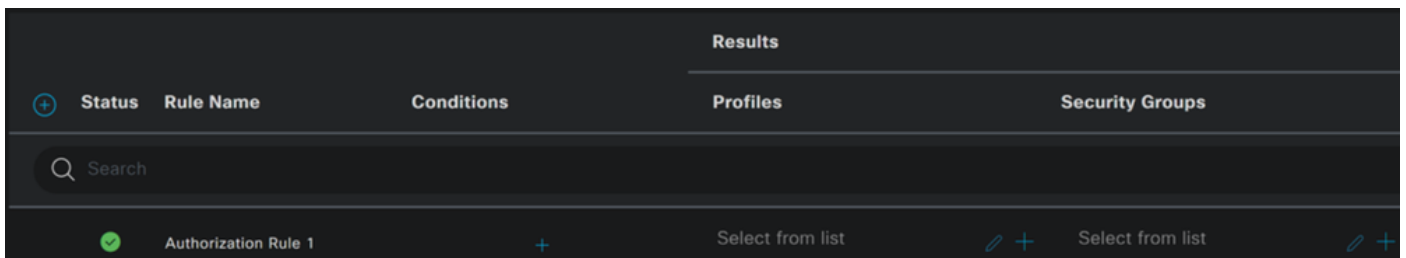


- Sous, cliquez **Profil** sur le bouton déroulant et sélectionnez le profil d'autorisation de réclamation configuré à l'étape [Profil d'autorisation de conformité](#)

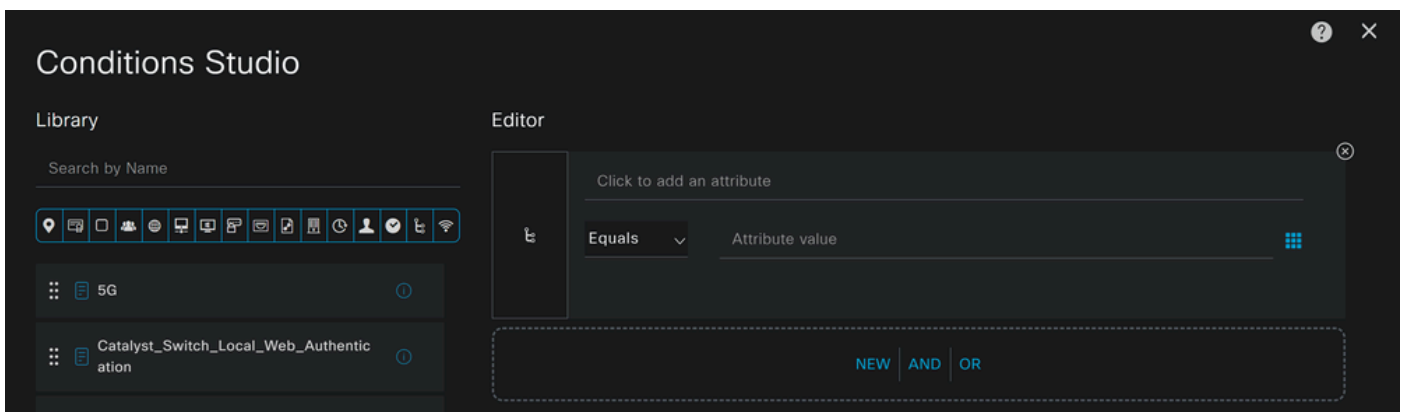


Vous venez de configurer le **Compliance Policy Set**.

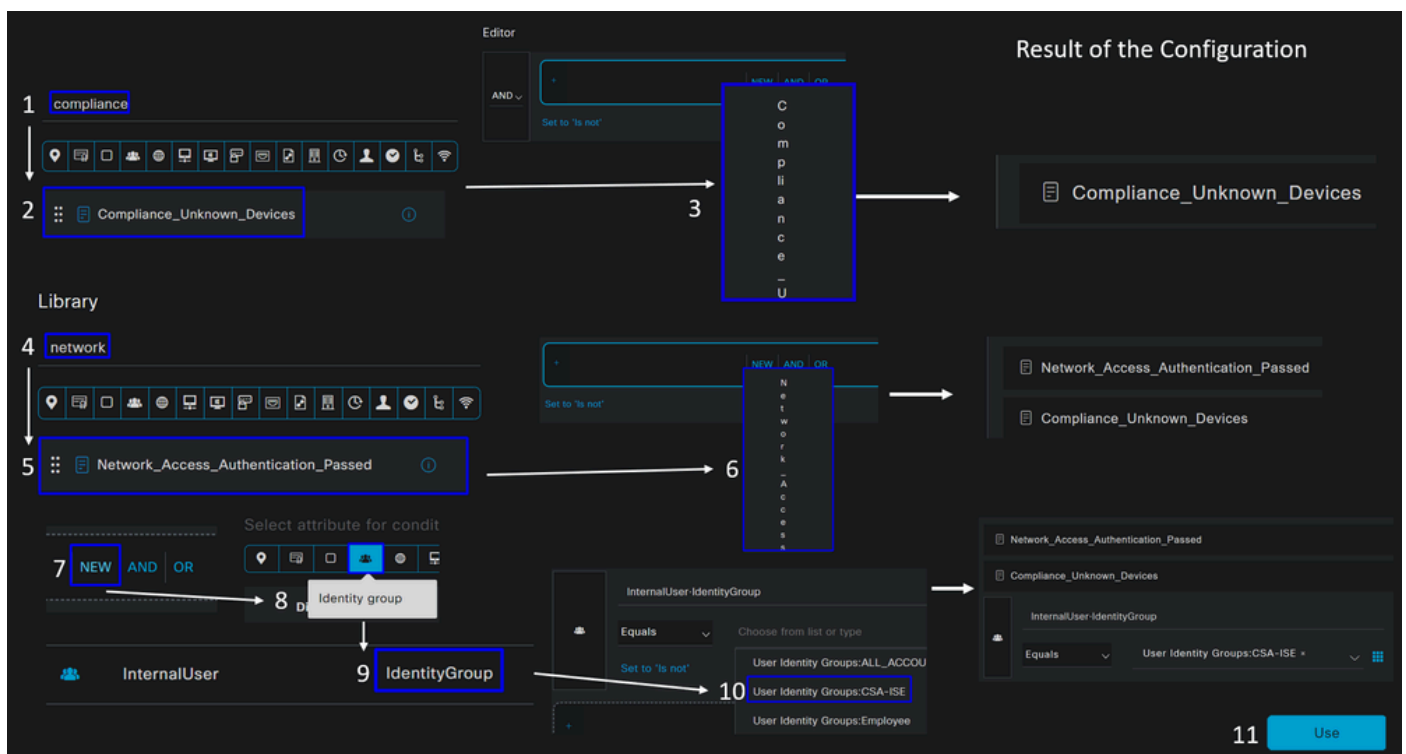
- Cliquez sur + pour définir la **CSA-Unknown-Compliance** politique :



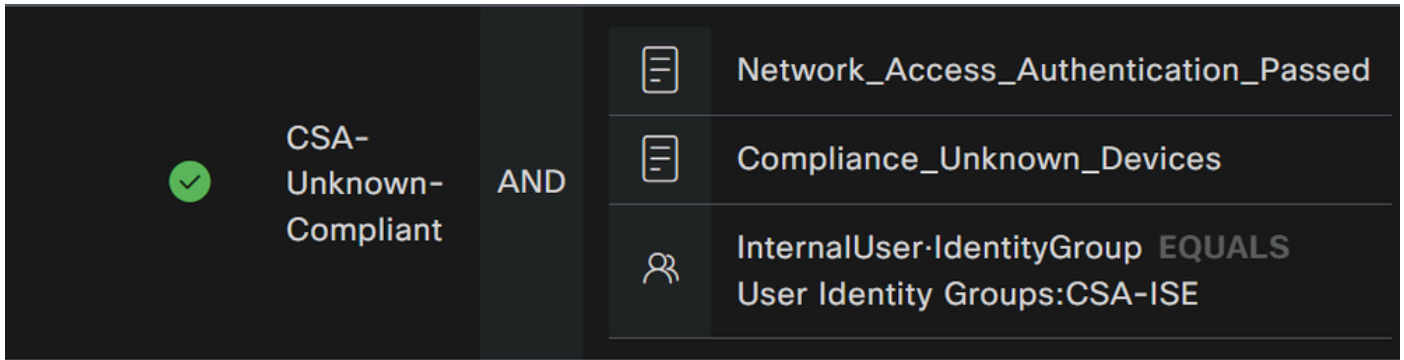
- Pour l'étape suivante, modifiez les Rule Name, Conditions et Profiles
- Lorsque vous définissez le paramètre **Name** configure a name sur **CSA-Unknown-Compliance**
- Pour configurer le **Condition**, cliquez sur le bouton +
- Sous **Condition Studio**, vous trouverez les informations suivantes :



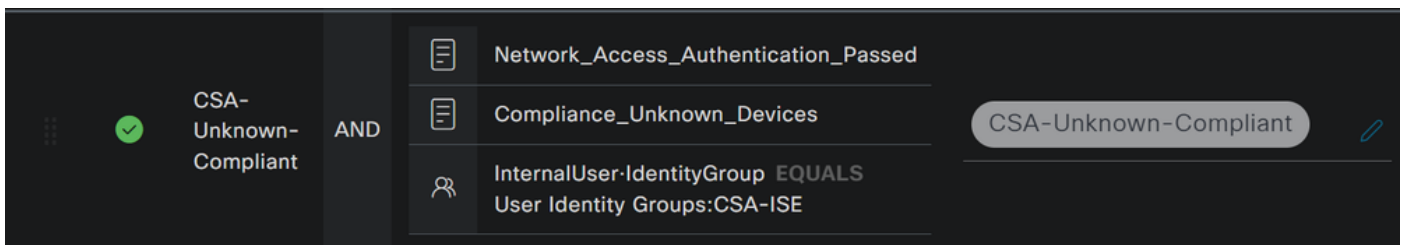
- Pour créer la condition, recherchez **compliance**
- Vous devez avoir affiché Compliant_Unknown_Devices
- Glisser-déplacer sous le **Editor**
- Pour créer la deuxième condition, recherchez **network**
- Vous devez avoir affiché Network_Access_Authentication_Passed
- Glisser-déplacer sous le **Editor**
- Cliquez sous la Editor dans **New**
- Cliquez sur l'**Identity Group** icône
- Choisir **Internal User Identity Group**
- Sous **Equals**, sélectionnez le **User Identity Group** que vous souhaitez faire correspondre
- Cliquer **Use**



- Par conséquent, vous obtenez l'image suivante

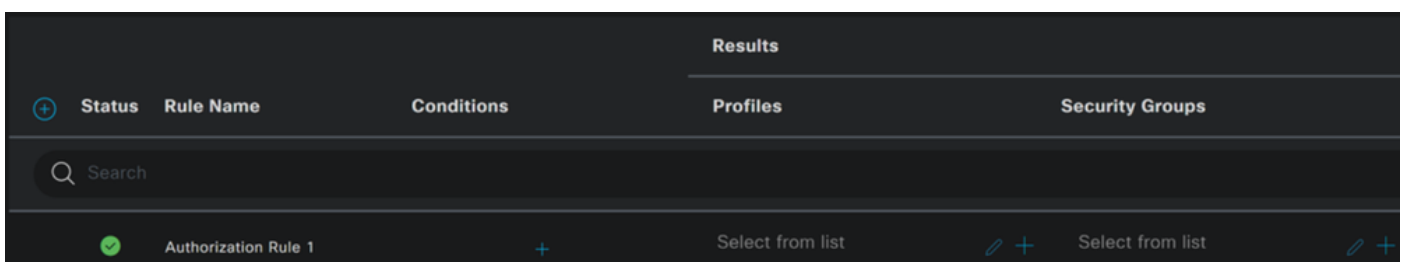


- Cliquez **Profile** sur le bouton déroulant et sélectionnez le profil d'autorisation de réclamation configuré à l'étape [Profil d'autorisation de conformité inconnu](#)



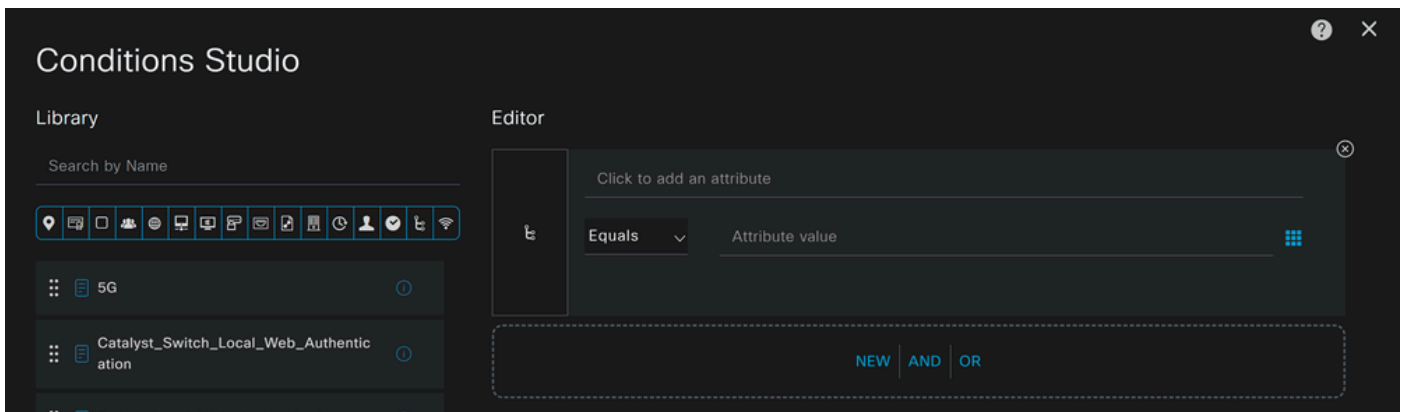
Vous venez de configurer le **Unknown Compliance Policy Set**.

- Cliquez sur + pour définir la **CSA- Non-Compliant** politique :

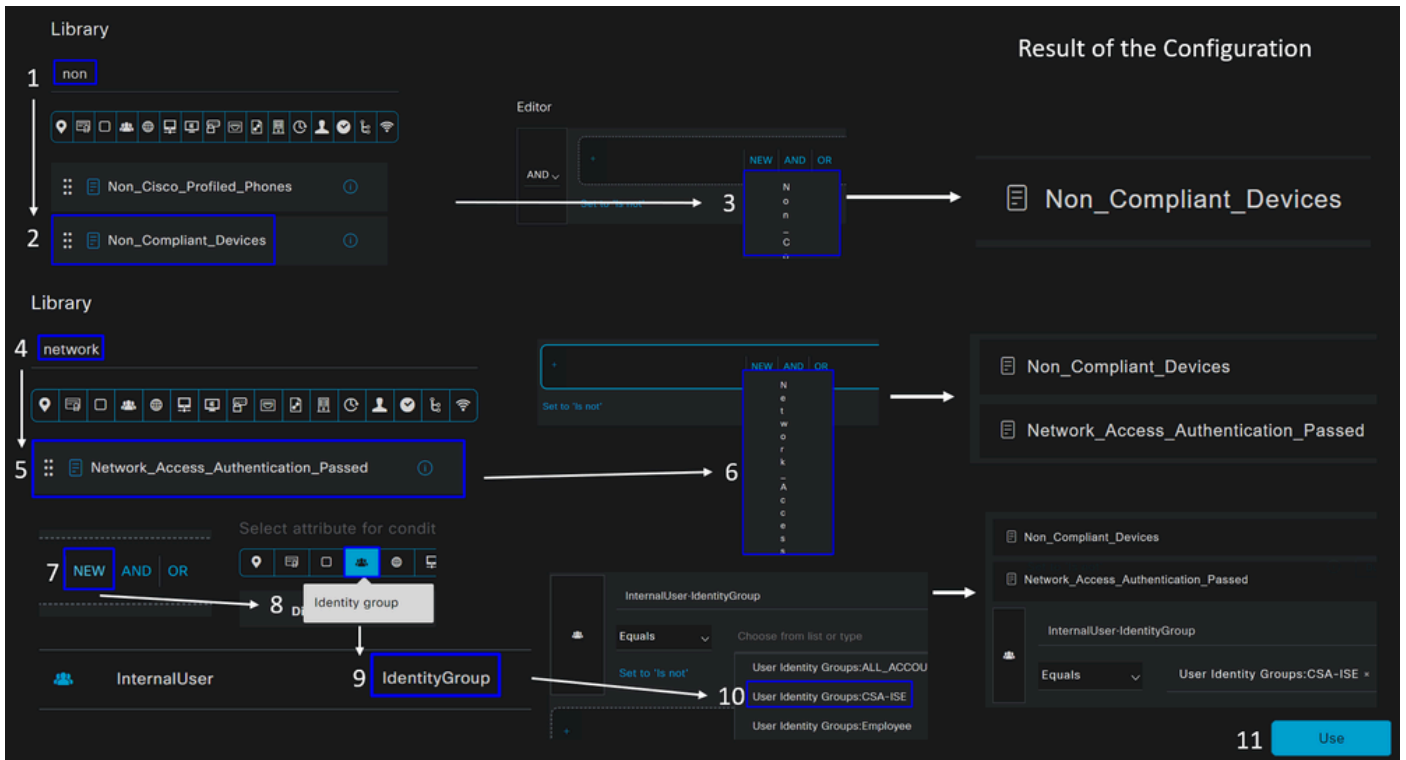


- Pour l'étape suivante, modifiez les Rule Name, Conditions et Profiles
- Lorsque vous définissez le paramètre **Name** configure a name sur **CSA-Non-Compliance**
- Pour configurer le **Condition**, cliquez sur le bouton +

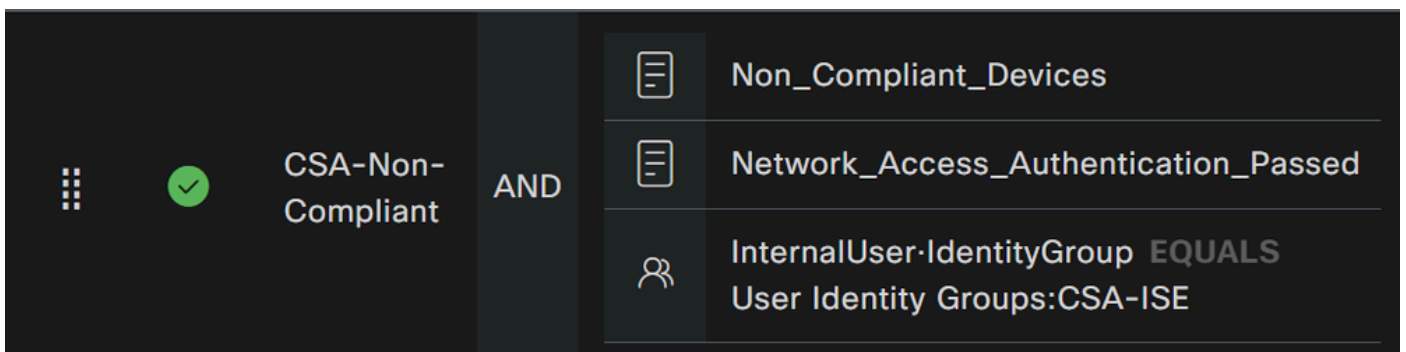
- Sous **Condition Studio**, vous trouverez les informations suivantes :



- Pour créer la condition, recherchez **non**
- Vous devez avoir affiché `Non_Compliant_Devices`
- Glisser-déplacer sous le **Editor**
- Pour créer la deuxième condition, recherchez **network**
- Vous devez avoir affiché `Network_Access_Authentication_Passed`
- Glisser-déplacer sous le **Editor**
- Cliquez sous la Editor dans **New**
- Cliquez sur l'**Identity Group** icône
- Choisir **Internal User Identity Group**
- Sous **Equals**, sélectionnez le **User Identity Group** que vous souhaitez faire correspondre
- Cliquer **Use**



- Par conséquent, vous obtenez l'image suivante



- Sous cliquez **Profile** sur le bouton déroulant et sélectionnez le profil d'autorisation de réclamation **DenyAccess**

CSA-Non-Compliant AND

- Non_Compliant_Devices
- Network_Access_Authentication_Passed
- InternalUser·IdentityGroup EQUALS User Identity Groups:CSA-ISE

DenyAccess

Une fois que vous avez terminé la configuration des trois profils, vous êtes prêt à tester votre intégration avec posture.

Vérifier

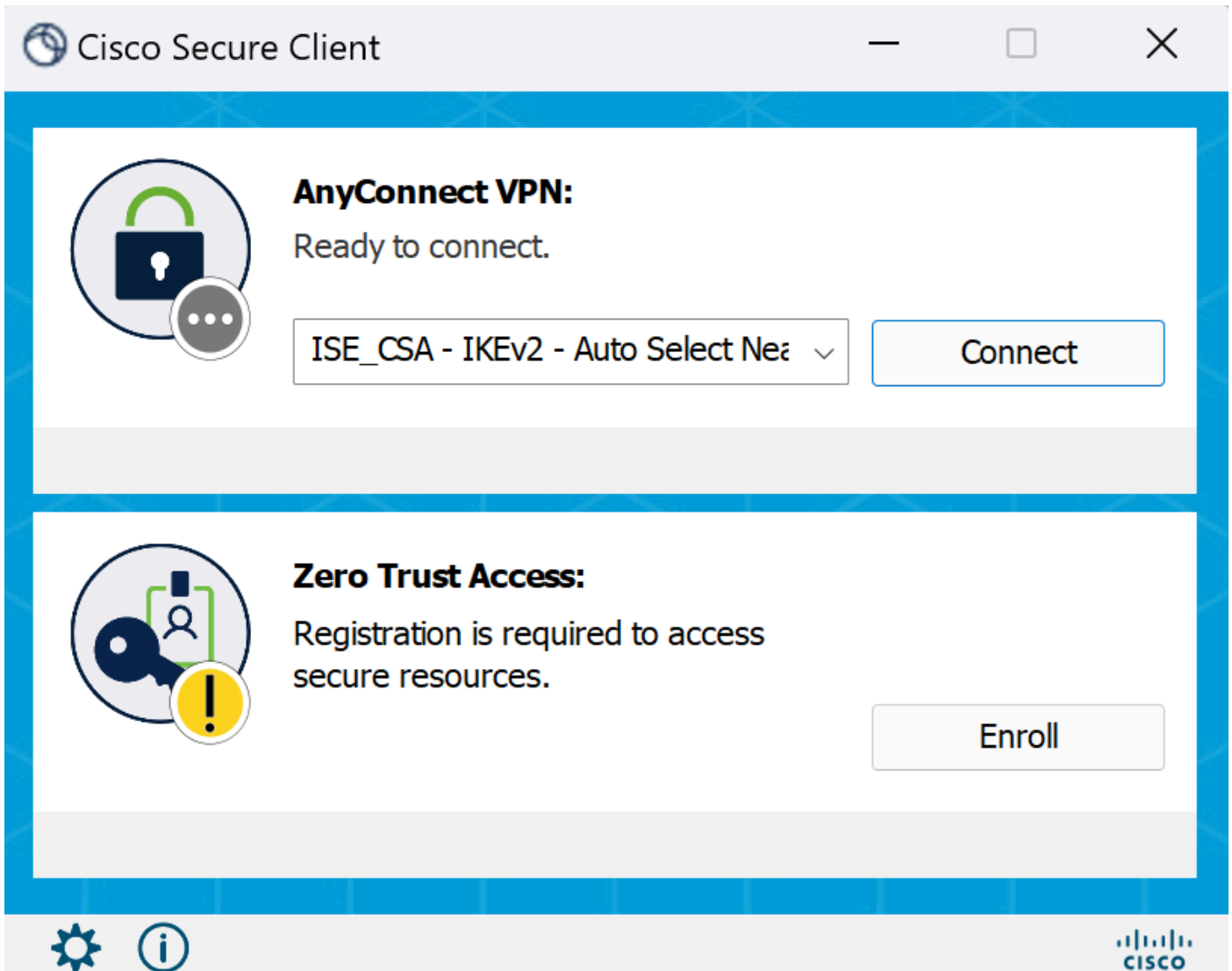
Validation de posture

Connexion sur l'ordinateur

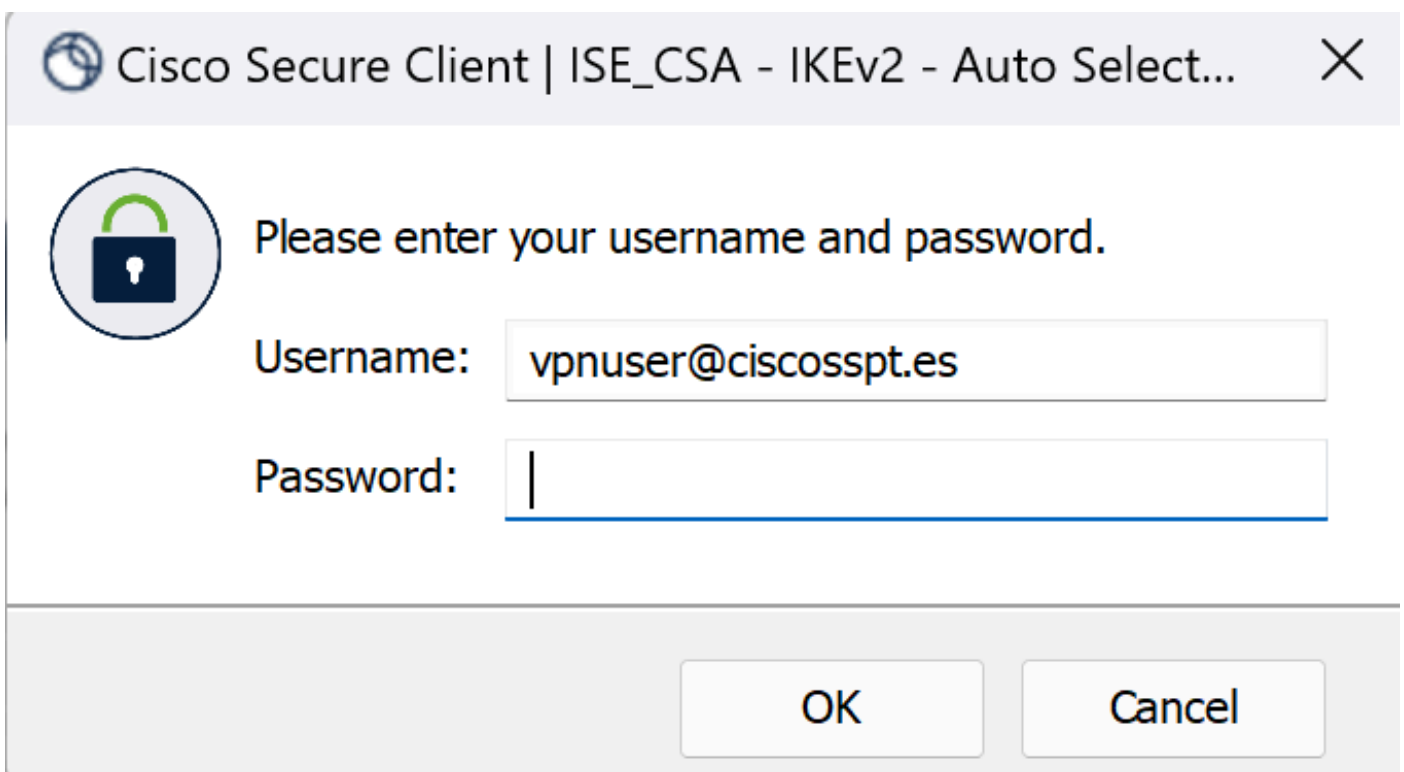
Connectez-vous à votre domaine FQDN RA-VPN fourni sur Secure Access via Secure Client.

Remarque : aucun module ISE ne doit être installé pour cette étape.

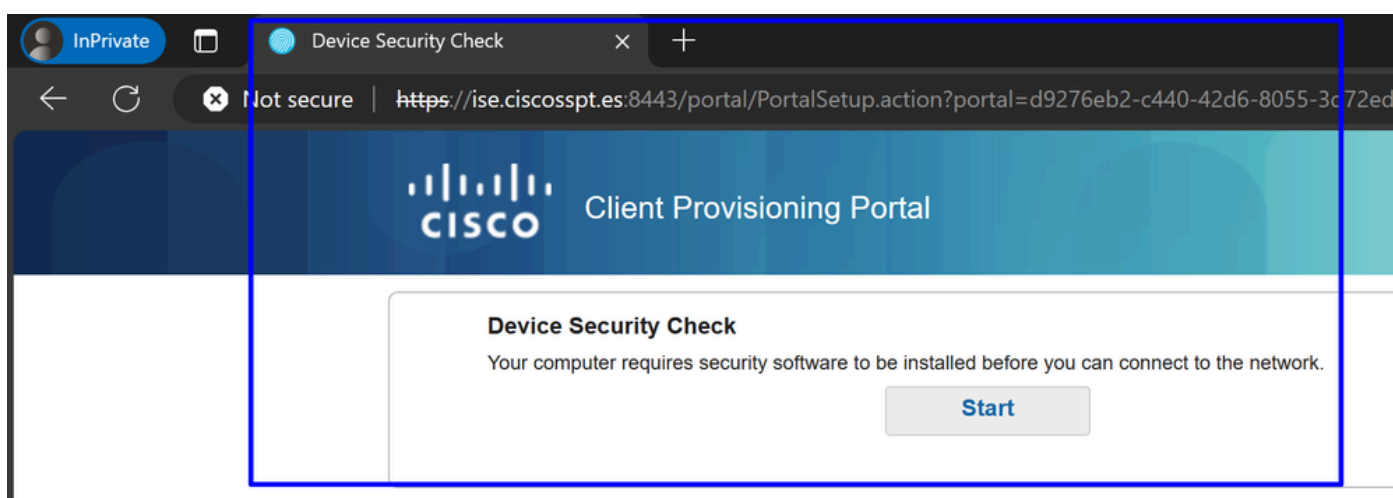
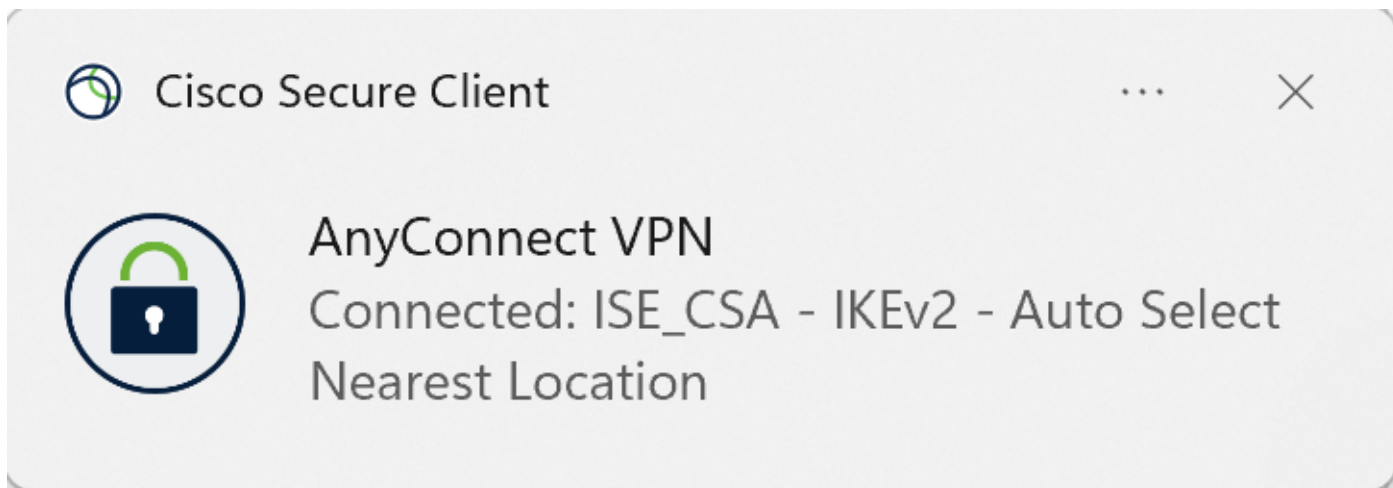
1. Connectez-vous à l'aide du client sécurisé.



2. Fournissez les informations d'identification afin de vous authentifier.



3. À ce stade, vous vous connectez au VPN, et la plupart du temps probablement, vous êtes redirigé vers ISE ; sinon, vous pouvez essayer de naviguer vers **http:1.1.1.1**.





Remarque : à ce stade, vous tombez sous l'autorisation - ensemble de stratégies [CSA-Unknown-Compliance](#) car vous n'avez pas installé l'agent de posture ISE sur la machine et vous êtes redirigé vers le portail de mise en service ISE pour installer l'agent.

4. Cliquez sur Démarrer pour poursuivre le provisionnement de l'agent.

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

9 Detecting if Agent is installed and running...

5. Cliquez sur + **This is my first time here.**

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent

+ + This is my first time here


+ + Remind me what to do next

6. Cliquez sur [Click here to download and install agent](#)

+ This is my first time here

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

 You have 4 minutes to install and for the compliance check to complete

7. Installer l'agent

Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

[See more](#)

Network Setup Assistant



Network Setup Assistant



Installation is completed.

Quit

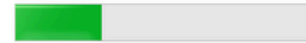
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. Une fois l'agent installé, la posture ISE commence à vérifier la posture actuelle des machines. Si les conditions de la stratégie ne sont pas remplies, une fenêtre contextuelle apparaît pour vous guider vers la conformité.



ISE Posture

1 Update(s) Required



30%

Time Remaining:

3 Minutes



Action Required to Enable Access

Updates are needed on your device before you can join the network.

This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details



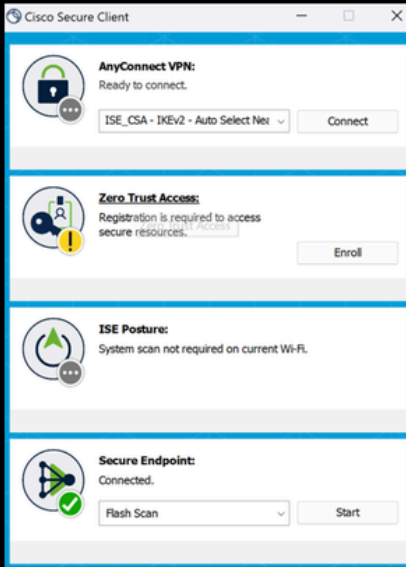
Cancel



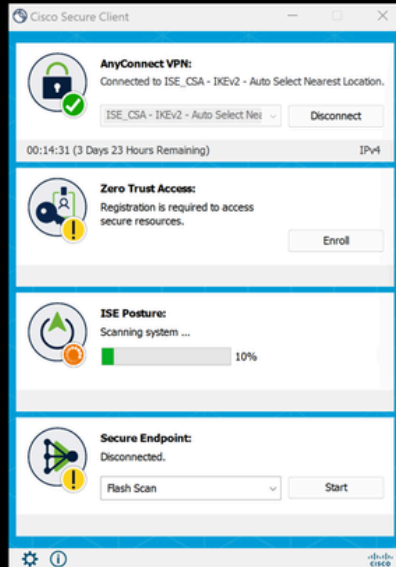
Remarque : si vous Cancel ou le temps restant se termine, vous devenez automatiquement non conforme, tombez sous le jeu de stratégies d'autorisation [CSA-Non-Compliance](#), et vous êtes immédiatement déconnecté du VPN.

9. Installez Secure Endpoint Agent et reconnectez-vous au VPN.

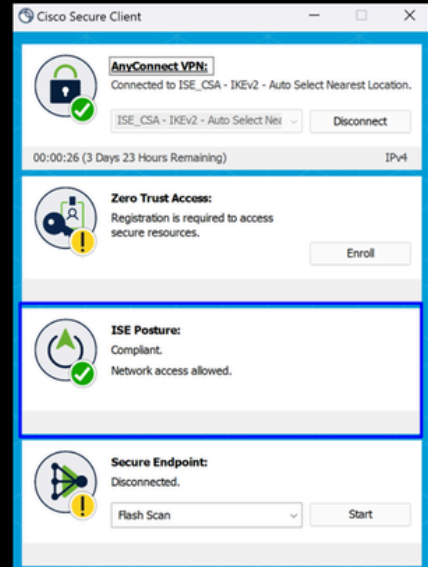
Secure Endpoint Installed



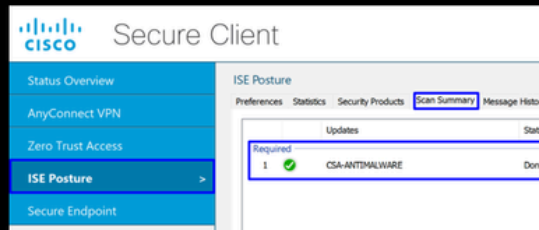
Agent Scanning



ISE Posture Successful validated



Scan Summary - Compliance



10. Une fois que l'agent a vérifié que la machine est conforme, votre position change pour être sur plainte et donner accès à toutes les ressources sur le réseau.



Remarque : une fois que vous êtes conforme, vous tombez sous le jeu de stratégies d'autorisation [CSA-Compliance](#), et vous avez immédiatement accès à toutes vos ressources réseau.

Comment collecter les journaux dans ISE

Pour vérifier le résultat de l'authentification d'un utilisateur, vous disposez de deux exemples de conformité et de non-conformité. Pour le consulter dans ISE, suivez les instructions suivantes :

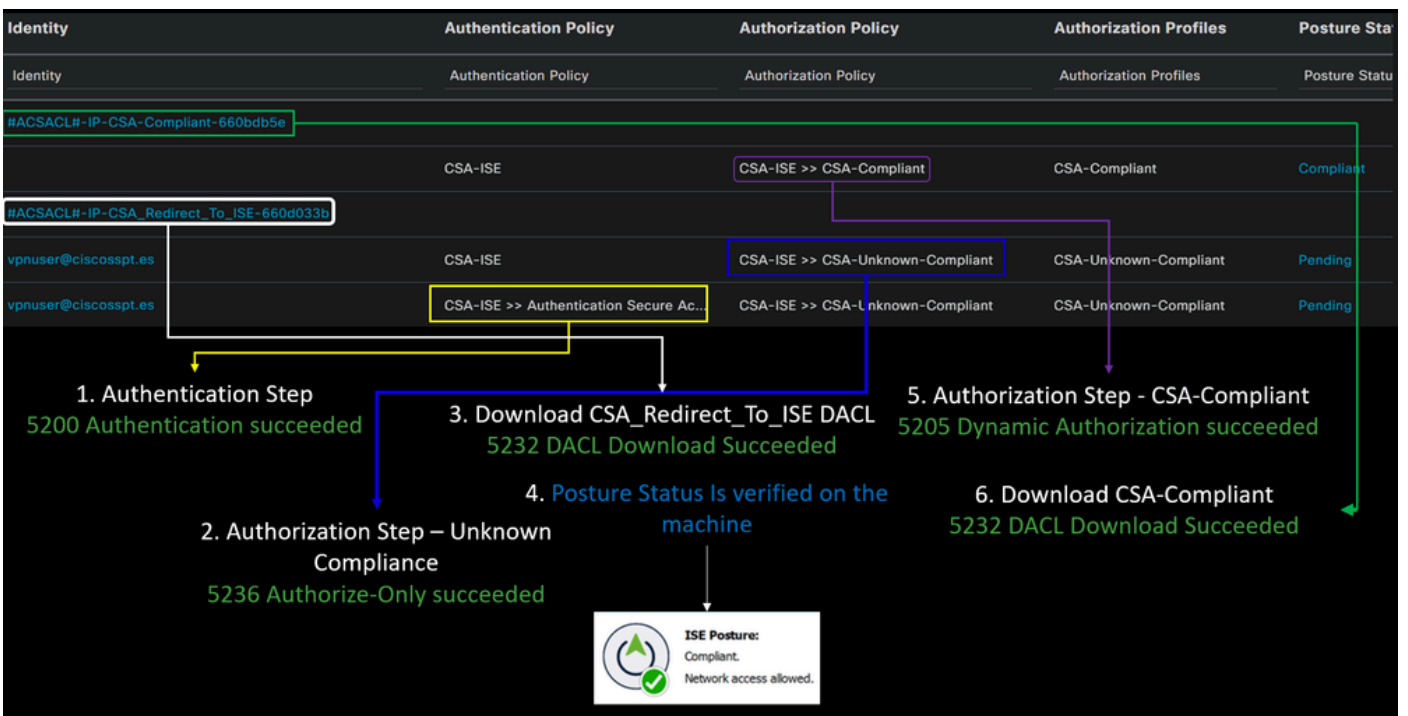
- Accédez à votre tableau de bord ISE

- Cliquez sur Operations > Live Logs

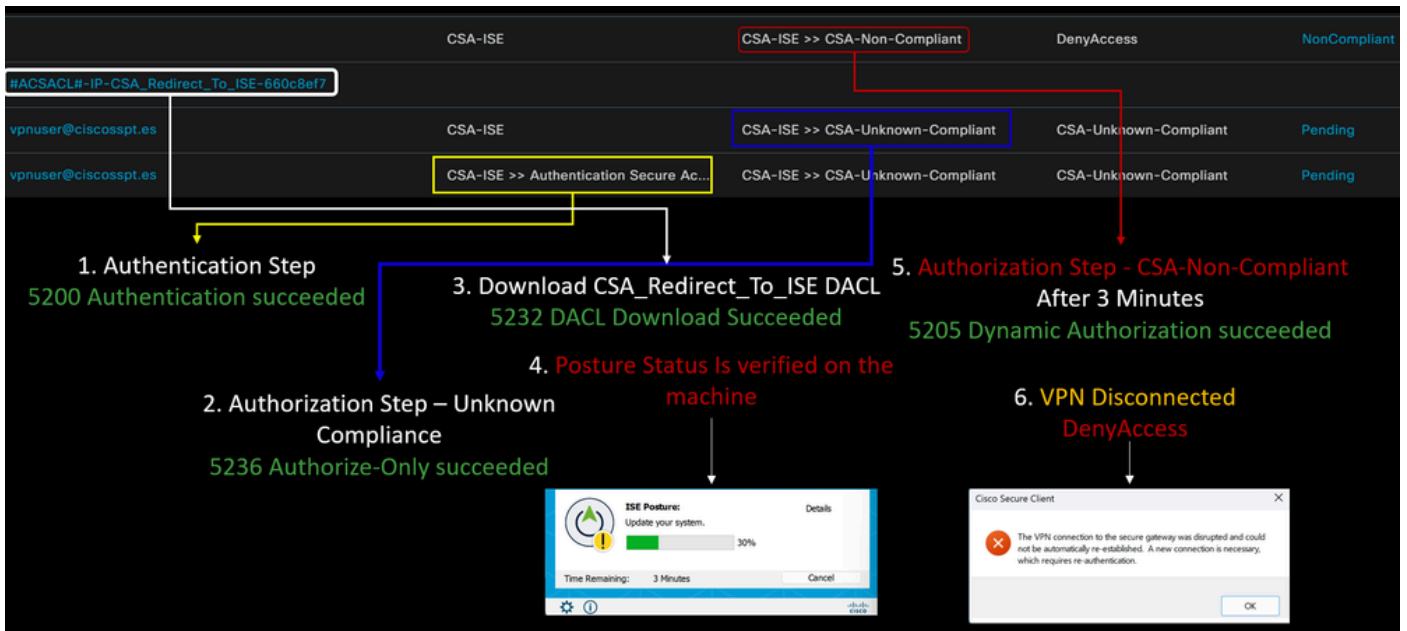
Misconfigured Suppliants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter	
0	0	0	0	0	
Refresh Never		Show Latest 50 records		Within Last 24 hours	
Reset Repeat Counts				Export To	
Filter					
Time	Status	Details	Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 07:00:27.7...	✓		Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 06:56:15.4...	✓		#ACSACL#-IP-CSA_Redirect_To_ISE-660d033b	CSA-ISE	CSA-ISE >> CSA-Non-Complia
Apr 03, 2024 06:56:15.3...	✓		vpuser@ciscospt.es	CSA-ISE	CSA-ISE >> CSA-Unknown-Co
Apr 03, 2024 06:56:15.2...	✓		vpuser@ciscospt.es	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> CSA-Unknown-Co

Le scénario suivant illustre l'affichage des événements de conformité et de non-conformité sous **Live Logs**:

Conformité



Non-conformité



Premiers pas avec l'accès sécurisé et l'intégration ISE

Dans l'exemple suivant, Cisco ISE se trouve sous le réseau 192.168.10.0/24 et la configuration des réseaux accessibles via le tunnel doit être ajoutée sous la configuration du tunnel.

Step 1: Vérifiez la configuration de votre tunnel :

Pour le vérifier, accédez à votre tableau de [bord d'accès sécurisé](#).

- Cliquez sur **Connect > Network Connections**
- Cliquez sur **Network Tunnel Groups > Votre tunnel**

HomeFTD	✓ Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-------------	------------------	---------------	---	---------------

- Sous summary, vérifiez que le tunnel a configuré l'espace d'adressage où se trouve votre Cisco ISE :

Summary



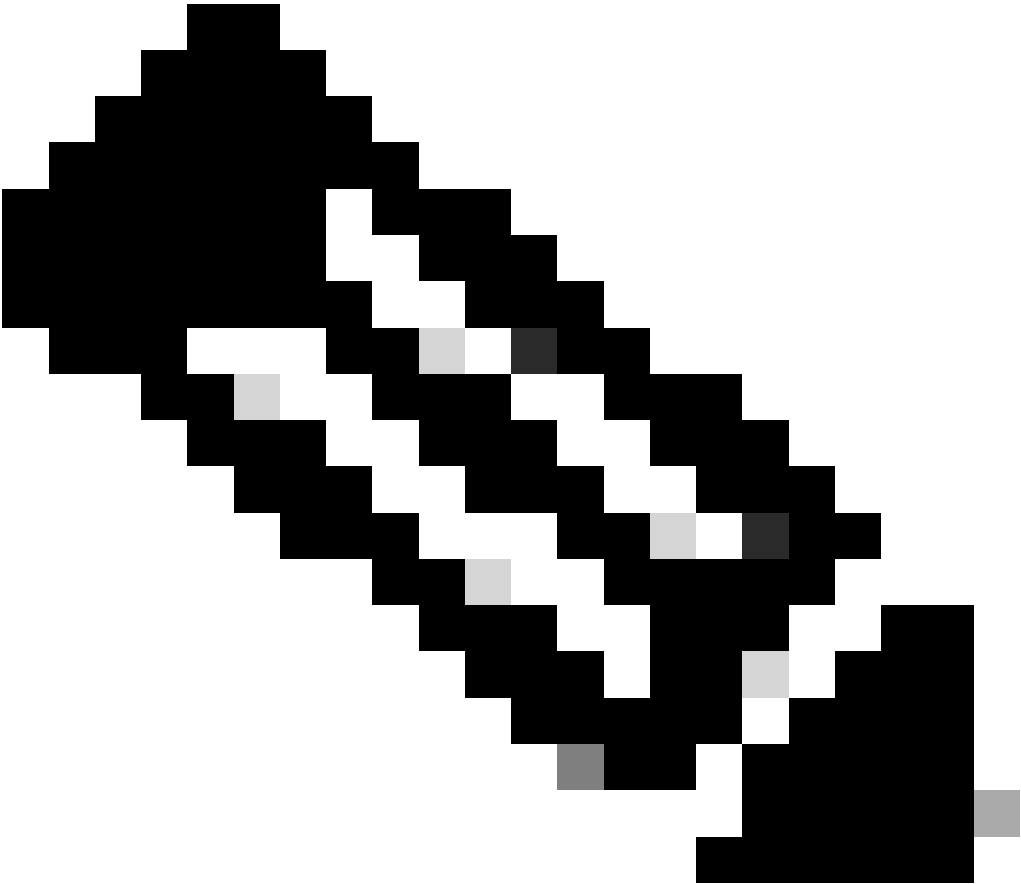
Connected

Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2: autorisez le trafic sur votre pare-feu.

Pour permettre à Secure Access d'utiliser votre périphérique ISE pour l'authentification Radius, vous devez avoir configuré une règle d'accès sécurisé à votre réseau avec les ports Radius requis :

Règle	Source	Destination	Port de destination
ISE pour un accès sécurisé Pool de gestion	Serveur_ISE	Pool IP de gestion (RA-VPN)	ACO UDP 1700 (port par défaut)
Pool IP de gestion d'accès sécurisé vers ISE	Pool IP de gestion	Serveur_ISE	Authentification, autorisation UDP 1812 (port par défaut) Gestion de comptes UDP 1813 (port par défaut)
Pool IP de terminaux d'accès sécurisé vers ISE	Pool d'adresses IP	Serveur_ISE	Provisioning Portal TCP 8443 (port par défaut)
Pool d'adresses IP de point d'accès sécurisé vers SERVEUR DNS	Pool d'adresses IP	Serveur DNS	DNS



Remarque : si vous souhaitez en savoir plus sur les ports liés à ISE, consultez le [Guide de l'utilisateur - Référence des ports](#).





Remarque : une règle DNS est nécessaire si vous avez configuré votre ISE pour qu'il soit détecté par un nom, tel que `ise.ciscospt.es`

Pool de gestion et pools IP de terminaux

Pour vérifier votre pool d'adresses IP de gestion et de terminaux, accédez à votre tableau de [bord d'accès sécurisé](#) :

- Cliquez sur **Connect > End User Connectivity**
- Cliquez sur Virtual Private Network

- Sous **Manage IP Pools**
- Cliquez sur **Manage**

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups	
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA	 

Étape 3 : vérifiez que votre ISE est configuré sous Ressources privées

Pour permettre aux utilisateurs connectés via le VPN de naviguer vers **ISE Provisioning Portal**, vous devez vous assurer que vous avez configuré votre périphérique en tant que ressource privée pour fournir l'accès, qui est utilisé pour permettre le provisionnement automatique du ISE Posture Module via le VPN.

Pour vérifier que vous avez configuré ISE correctement, accédez à votre tableau de [bord d'accès sécurisé](#) :

- Cliquez sur **Resources > Private Resources**
- Cliquez sur la ressource ISE

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#) 

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ Protocol & Port](#)

[+ IP Address or FQDN](#)

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

Si nécessaire, vous pouvez limiter la règle au port du portail d'approvisionnement (8443).



Remarque : assurez-vous d'avoir coché la case correspondant aux connexions VPN.

Étape 4 : Autorisez l'accès ISE dans le cadre de la stratégie d'accès

Pour autoriser les utilisateurs connectés via le VPN à accéder à **ISE Provisioning Portal**, vous devez être sûr d'avoir configuré et **Access Policy** d'autoriser les utilisateurs configurés sous cette règle à accéder à la ressource privée configurée dans Step3.

Pour vérifier que vous avez configuré ISE correctement, accédez à votre tableau de [bord d'accès sécurisé](#) :



- Cliquez sur **Secure > Access Policy**

- Cliquez sur la règle configurée pour autoriser l'accès des utilisateurs VPN à ISE

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)


Action

 Allow Allow specified traffic if security requirements are met.	 Block Block specified traffic.
---	--


From Specify one or more sources . <input type="text" value="CSA (ciscospt.es\CSA)"/>	To Specify one or more destinations . <input type="text" value="CiscoSE"/>
Information about sources, including selecting multiple sources. Help	Information about destinations, including selecting multiple destinations. Help

Endpoint Requirements

For VPN connections:

-  End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. [?](#)
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

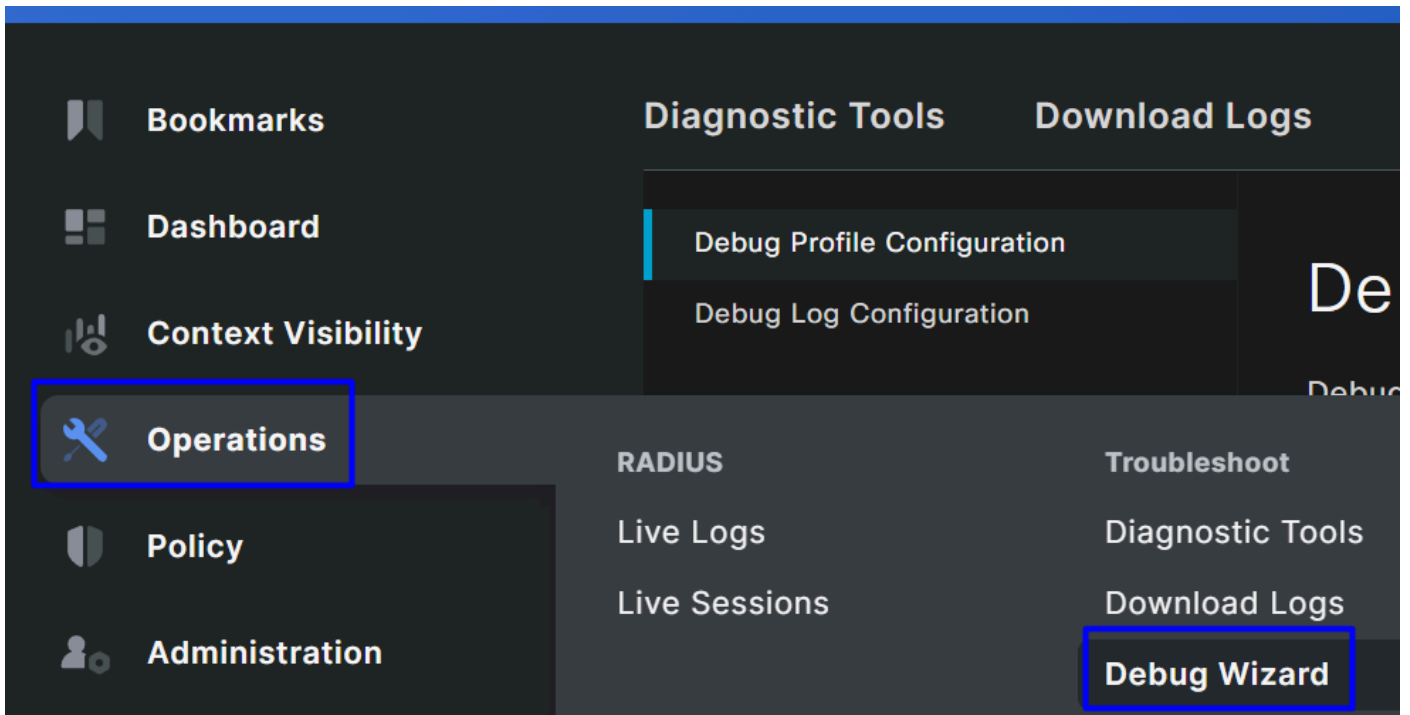
-  Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

Dépannage

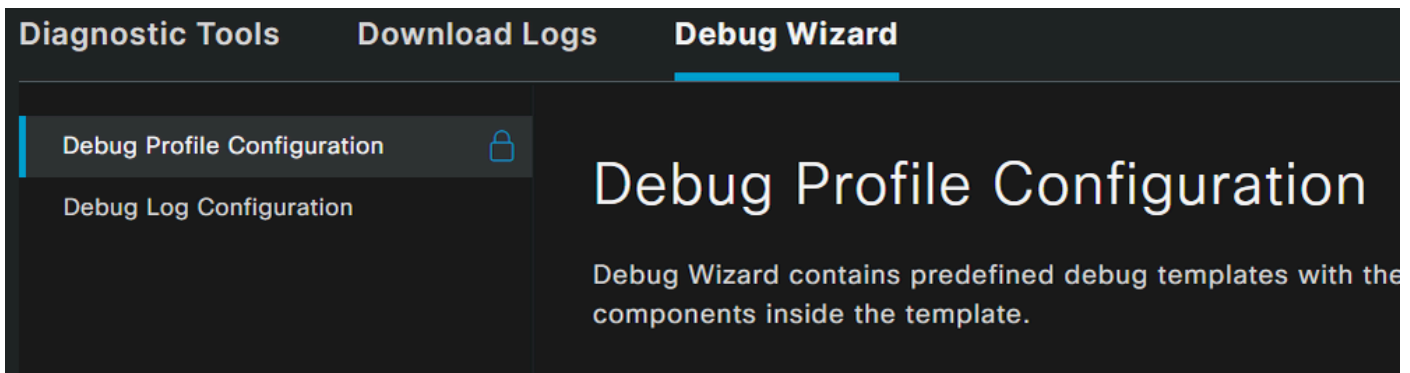
Téléchargement des journaux de débogage de la position ISE

Pour télécharger les journaux ISE afin de vérifier un problème lié à la position, procédez comme suit :

- Accédez à votre tableau de bord ISE
- Cliquez sur **Operations > Troubleshoot > Debug Wizard**



- Cliquez sur Debug Profile Configuration



- Cochez la case correspondant à **Posture > Debug Nodes**



Add



Edit



Remove 2



Debug Nodes



Name

Des



802.1X/MAB

802



Active Directory

Acti



Application Server Issues

App



BYOD portal/Onboarding

BYO



Context Visibility

Con



Guest portal

Gue



Licensing

Lice



MnT

MnT

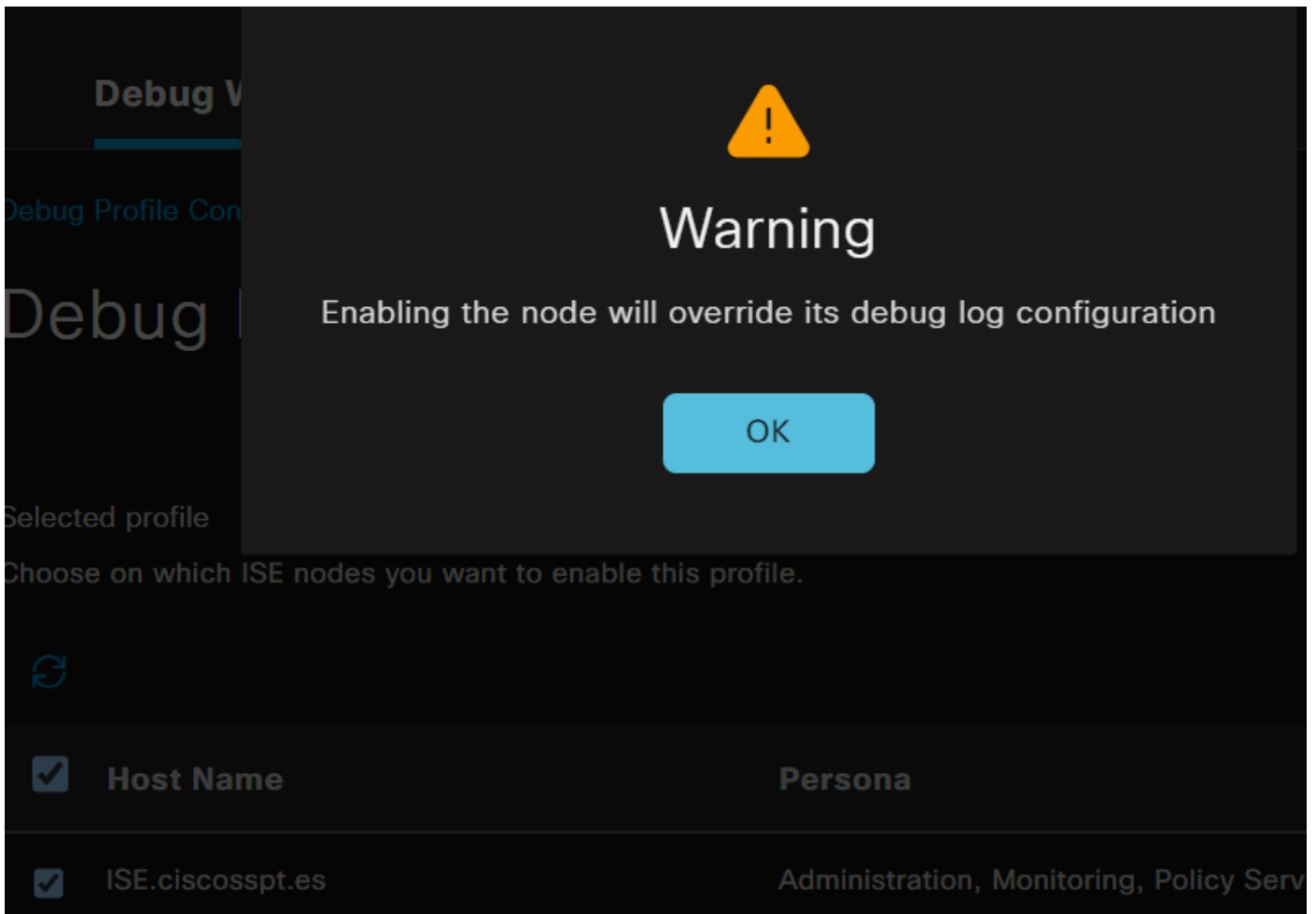
1



Posture

Pos

- Cochez la case des noeuds ISE sur lesquels vous devez activer le mode de débogage pour résoudre votre problème



The image shows a dark-themed user interface with a central warning dialog box. The dialog box has a yellow warning triangle icon at the top, followed by the word "Warning" in large white text. Below this, the message "Enabling the node will override its debug log configuration" is displayed in white. At the bottom of the dialog is a blue "OK" button. In the background, a table is partially visible with a "Host Name" column and a "Persona" column. The first row shows "ISE.ciscosspt.es" under "Host Name" and "Administration, Monitoring, Policy Serv" under "Persona". A blue refresh icon is located to the left of the table.

Host Name	Persona
<input checked="" type="checkbox"/> ISE.ciscosspt.es	Administration, Monitoring, Policy Serv

- Cliquer Save

Debug Nodes

Selected profile Posture

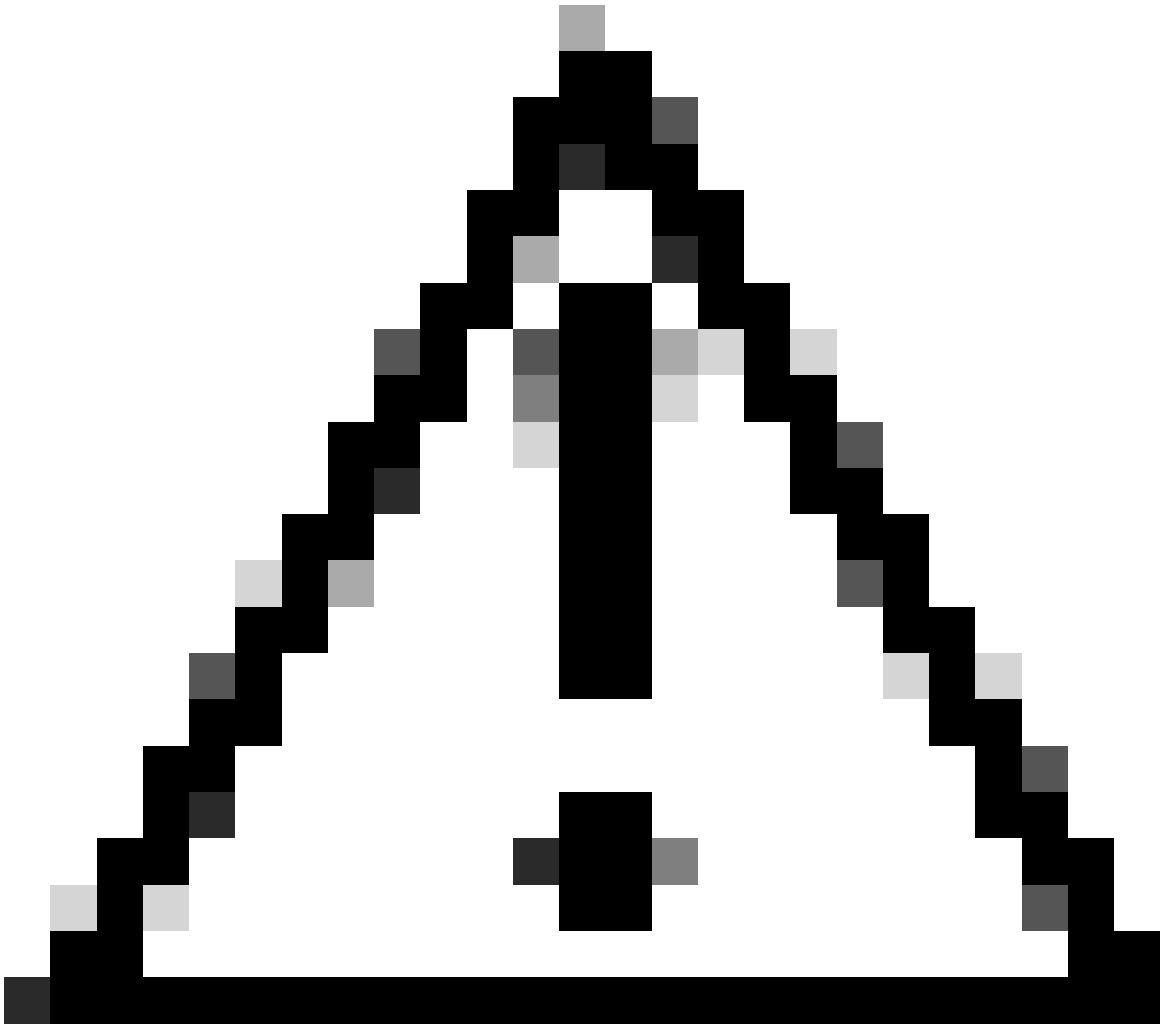
Choose on which ISE nodes you want to enable this profile.

 Filter  

<input checked="" type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> ISE.ciscosppt.es	Administration, Monitoring, Policy Service	STANDALONE

Cancel

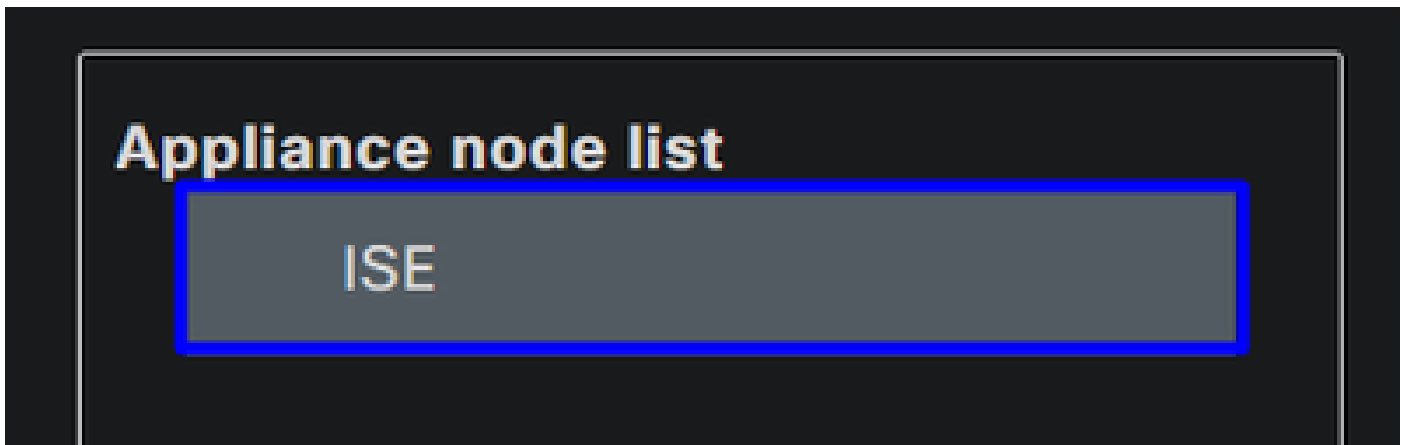
Save



Attention : après ce point, vous devez commencer à reproduire votre problème ; **the debug logs can affect the performance of your device.**

Une fois le problème reproduit, passez aux étapes suivantes :

- Cliquez sur Operations > Download Logs
- Sélectionnez le noeud à partir duquel vous voulez prendre les journaux



- Sous **Support Bundle**, choisissez les options suivantes :

Support Bundle

Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- Include debug logs
- Sous **Support Bundle Encryption**
 - **Shared Key Encryption**
 - Remplir **Encryption key** et **Re-Enter Encryption key**

- Cliquer **Create Support Bundle**
- Cliquer **Download**

✓ Support Bundle - Last Generated

File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

Download

Delete


















Avertissement : désactivez le mode de débogage activé à l'étape [Configuration du profil de débogage](#)

Vérification des journaux d'accès à distance Secure Access

Accédez à votre tableau de bord Secure Access :

- Cliquez sur Monitor > Remote Access Logs

100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

Générer un bundle DART sur le client sécurisé

Pour générer un bundle DART sur votre machine, vérifiez l'article suivant :

[Outil Cisco Secure Client Diagnostic and Reporting Tool \(DART\)](#)



Remarque : une fois que vous avez collecté les journaux indiqués dans la section de dépannage, ouvrez un dossier avec **TAC** pour poursuivre l'analyse des informations.

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Documentation et guide de l'utilisateur Secure Access](#)

- [Téléchargement du logiciel Cisco Secure Client](#)
- [Guide de l'administrateur de Cisco Identity Services Engine, version 3.3](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.